may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case the user, at his own expense, will be required to take whatever measures may be required to correct the interference.

Any modifications to this device, unless expressly approved by the manufacturer, can void the user's authority to operate this equipment under part 15 of the FCC rules.

**Canadian Regulatory Compliance**

This class A digital apparatus complies with Canadian I CES-003.

**Standards Compliance**

This product conforms to the IEC, European Union, ANSI/UL and Canadian CSA standards applicable to Information Technology products at the time of manufacture.

**Acknowledgments**

This product includes software developed by the University of California, Berkeley and its contributors.

This product includes software developed by the Computer Systems Engineering Group at the Lawrence Berkeley Laboratory.

This product includes software developed by the NetBSD Foundation, Inc. and its contributors.

This product includes software developed by Christopher G. Demetriou for the NetBSD Project.

This product includes software developed by Adam Glass.

This product includes software developed by Christian E. Hopps.

This product includes software developed by Dean Huxley.

This product includes software developed by John Kohl.

This product includes software developed by Paul Kranenburg.

This product includes software developed by Terrence R. Lambert.

This product includes software developed by Philip A. Nelson.

This product includes software developed by Herb Peyerl.

This product includes software developed by Jochen Pohl for the NetBSD Project.

This product includes software developed by Chris Provenzano.

This product includes software developed by Theo de Raadt.

This product includes software developed by David Muir Sharnoff.

This product includes software developed by SigmaSoft, Th. Lockert.

This product includes software developed for the NetBSD Project by Jason R. Thorpe.

This product includes software developed by Jason R. Thorpe for And Communications, http://www.and.com.

This product includes software developed for the NetBSD Project by Frank Van der Linden.

This product includes software developed for the NetBSD Project by John M. Vinopal.

This product includes software developed by Christos Zoulas.

This product includes software developed by Charles Hannum.

This product includes software developed by Charles Hannum, by the University of Vermont and State Agricultural College and Garrett A. Wollman, by William F. Jolitz, and by the University of California, Berkeley, Lawrence Berkeley Laboratory, and its contributors.

This product includes software developed by the University of Vermont and State Agricultural College and Garrett A. Wollman.

In the following statement, “This software” refers to the Mitsumi CD-ROM driver: This software was developed by Holger Veit and Brian Moore for use with “386BSD” and similar operating systems. “Similar operating systems” includes mainly non-profit oriented systems for research and education, including but not restricted to “NetBSD,” “FreeBSD,” “Mach” (by CMU).

In the following statement, “This software” refers to the parallel port driver: This software is a component of “386BSD” developed by William F. Jolitz, TeleMuse.

This product includes software developed by the Apache Group for use in the Apache HTTP server project (http://www.apache.org/).

This product includes software developed by Darren Reed. (© 1993–1998 by Darren Reed).
This product includes software licensed from Richard H. Porter under the GNU Library General Public License (© 1998, Red Hat Software), www.gnu.org/copyleft/lgpl.html.

This product includes the standard version of Perl software licensed under the Perl Artistic License (© 1997, 1998 Tom Christiansen and Nathan Torkington). All rights reserved. You may find the most current standard version of Perl at http://www.perl.com.
Table of Contents
# Traffic Management Shell (tmsh) Reference Guide

## 1 Introducing the Traffic Management Shell

<table>
<thead>
<tr>
<th>About the Traffic Management Shell</th>
<th>1-1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Additional command line utilities and tools</td>
<td>1-2</td>
</tr>
<tr>
<td>Basic syntax conventions</td>
<td>1-3</td>
</tr>
</tbody>
</table>

## 2 Understanding and Using the Traffic Management Shell

<table>
<thead>
<tr>
<th>Using tmsh</th>
<th>2-2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Loading and saving the system configuration</td>
<td>2-2</td>
</tr>
<tr>
<td>Working within the tmsh hierarchy</td>
<td>2-3</td>
</tr>
<tr>
<td>Using the scripting feature</td>
<td>2-6</td>
</tr>
<tr>
<td>Using the command completion feature</td>
<td>2-7</td>
</tr>
<tr>
<td>Using the help feature</td>
<td>2-8</td>
</tr>
<tr>
<td>Using the context-sensitive help feature</td>
<td>2-9</td>
</tr>
<tr>
<td>Interrupting a command</td>
<td>2-9</td>
</tr>
<tr>
<td>Entering multiple commands</td>
<td>2-10</td>
</tr>
<tr>
<td>Using the command glob feature</td>
<td>2-10</td>
</tr>
<tr>
<td>Using the command audit feature</td>
<td>2-14</td>
</tr>
<tr>
<td>Using the command aliases feature</td>
<td>2-16</td>
</tr>
<tr>
<td>Using the wildcard search feature</td>
<td>2-18</td>
</tr>
<tr>
<td>Using the statistics feature</td>
<td>2-18</td>
</tr>
<tr>
<td>Using grep functionality in tmsh to filter output</td>
<td>2-21</td>
</tr>
<tr>
<td>Creating batch mode transactions</td>
<td>2-22</td>
</tr>
<tr>
<td>Controlling tmsh</td>
<td>2-23</td>
</tr>
<tr>
<td>Introduction to command syntax</td>
<td>2-26</td>
</tr>
</tbody>
</table>

## 3 Global Commands

<table>
<thead>
<tr>
<th>Introducing global commands</th>
<th>3-1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alphabetical list of global commands</td>
<td>3-1</td>
</tr>
<tr>
<td>cd</td>
<td>3-2</td>
</tr>
<tr>
<td>cp</td>
<td>3-4</td>
</tr>
<tr>
<td>create</td>
<td>3-6</td>
</tr>
<tr>
<td>delete</td>
<td>3-8</td>
</tr>
<tr>
<td>edit</td>
<td>3-10</td>
</tr>
<tr>
<td>exit</td>
<td>3-13</td>
</tr>
<tr>
<td>generate</td>
<td>3-14</td>
</tr>
<tr>
<td>help</td>
<td>3-15</td>
</tr>
<tr>
<td>install</td>
<td>3-17</td>
</tr>
<tr>
<td>list</td>
<td>3-18</td>
</tr>
<tr>
<td>load</td>
<td>3-21</td>
</tr>
<tr>
<td>modify</td>
<td>3-22</td>
</tr>
<tr>
<td>mv</td>
<td>3-24</td>
</tr>
<tr>
<td>publish</td>
<td>3-26</td>
</tr>
<tr>
<td>pwd</td>
<td>3-27</td>
</tr>
<tr>
<td>quit</td>
<td>3-28</td>
</tr>
<tr>
<td>reboot</td>
<td>3-29</td>
</tr>
<tr>
<td>reset-stats</td>
<td>3-31</td>
</tr>
<tr>
<td>restart</td>
<td>3-33</td>
</tr>
<tr>
<td>run</td>
<td>3-34</td>
</tr>
<tr>
<td>save</td>
<td>3-37</td>
</tr>
<tr>
<td>send-mail</td>
<td>3-38</td>
</tr>
</tbody>
</table>
## Table of Contents

### 9  
apm policy agent Module Components

<table>
<thead>
<tr>
<th>Component</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introducing the apm policy agent module</td>
<td>9-1</td>
</tr>
<tr>
<td>Alphabetical list of components</td>
<td>9-1</td>
</tr>
<tr>
<td>aaa-active-directory</td>
<td>9-2</td>
</tr>
<tr>
<td>aaa-client-cert</td>
<td>9-6</td>
</tr>
<tr>
<td>aaa-crdlp</td>
<td>9-8</td>
</tr>
<tr>
<td>aaa-http</td>
<td>9-10</td>
</tr>
<tr>
<td>aaa-ldap</td>
<td>9-12</td>
</tr>
<tr>
<td>aaa-ocsp</td>
<td>9-15</td>
</tr>
<tr>
<td>aaa-radius</td>
<td>9-17</td>
</tr>
<tr>
<td>aaa-securid</td>
<td>9-19</td>
</tr>
<tr>
<td>acct-radius</td>
<td>9-21</td>
</tr>
<tr>
<td>acct-tacacsplus</td>
<td>9-23</td>
</tr>
<tr>
<td>decision-box</td>
<td>9-25</td>
</tr>
<tr>
<td>dynamic-act</td>
<td>9-27</td>
</tr>
<tr>
<td>ending-allow</td>
<td>9-29</td>
</tr>
<tr>
<td>ending-deny</td>
<td>9-31</td>
</tr>
<tr>
<td>ending-redirect</td>
<td>9-33</td>
</tr>
<tr>
<td>endpoint-check-av</td>
<td>9-35</td>
</tr>
<tr>
<td>endpoint-check-fw</td>
<td>9-38</td>
</tr>
<tr>
<td>endpoint-linux-check-file</td>
<td>9-41</td>
</tr>
<tr>
<td>endpoint-linux-check-process</td>
<td>9-44</td>
</tr>
<tr>
<td>endpoint-mac-check-file</td>
<td>9-46</td>
</tr>
<tr>
<td>endpoint-mac-check-process</td>
<td>9-49</td>
</tr>
<tr>
<td>endpoint-windows-browser-cache-cleaner</td>
<td>9-51</td>
</tr>
<tr>
<td>endpoint-windows-check-file</td>
<td>9-54</td>
</tr>
<tr>
<td>endpoint-windows-check-machine-cert</td>
<td>9-58</td>
</tr>
<tr>
<td>endpoint-windows-check-process</td>
<td>9-61</td>
</tr>
<tr>
<td>endpoint-windows-check-registry</td>
<td>9-63</td>
</tr>
<tr>
<td>endpoint-windows-group-policy</td>
<td>9-66</td>
</tr>
<tr>
<td>endpoint-windows-info-os</td>
<td>9-68</td>
</tr>
<tr>
<td>endpoint-windows-machine-info</td>
<td>9-70</td>
</tr>
<tr>
<td>endpoint-windows-protected-workspace</td>
<td>9-72</td>
</tr>
<tr>
<td>external-logon-page</td>
<td>9-74</td>
</tr>
<tr>
<td>irule-event</td>
<td>9-76</td>
</tr>
<tr>
<td>kerberos</td>
<td>9-79</td>
</tr>
<tr>
<td>logging</td>
<td>9-81</td>
</tr>
<tr>
<td>logon-page</td>
<td>9-83</td>
</tr>
<tr>
<td>message-box</td>
<td>9-87</td>
</tr>
<tr>
<td>oam</td>
<td>9-89</td>
</tr>
<tr>
<td>resource-assign</td>
<td>9-92</td>
</tr>
<tr>
<td>route-domain-selection</td>
<td>9-95</td>
</tr>
<tr>
<td>tacacsplus</td>
<td>9-97</td>
</tr>
<tr>
<td>variable-assign</td>
<td>9-99</td>
</tr>
</tbody>
</table>

### 10  
apm profile Module Components

<table>
<thead>
<tr>
<th>Component</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introducing the apm profile module</td>
<td>10-1</td>
</tr>
<tr>
<td>Alphabetical list of components</td>
<td>10-1</td>
</tr>
<tr>
<td>access</td>
<td>10-2</td>
</tr>
<tr>
<td>connectivity</td>
<td>10-8</td>
</tr>
<tr>
<td>remote-desktop</td>
<td>10-13</td>
</tr>
<tr>
<td>rewrite</td>
<td>10-14</td>
</tr>
</tbody>
</table>
Table of Contents

11

apm resource Module Components

Introducing the apm resource module ................................................................. 11-1
Alphabetical list of components ........................................................................... 11-1
app-tunnel .............................................................................................................. 11-2
client-rate-class .................................................................................................. 11-5
client-traffic-classifier ........................................................................................ 11-9
ipv6-leasepool ...................................................................................................... 11-12
leasepool ............................................................................................................... 11-14
network-access .................................................................................................... 11-16
portal-access ....................................................................................................... 11-24
webtop .................................................................................................................. 11-28
webtop-link .......................................................................................................... 11-31

12

apm resource remote-desktop Module Components

Introducing the apm resource remote-desktop module ........................................ 12-1
Alphabetical list of components ........................................................................... 12-1
citrix ..................................................................................................................... 12-2
citrix-client-bundle ............................................................................................ 12-6
citrix-client-package-file ...................................................................................... 12-8
rdp .......................................................................................................................... 12-10

13

apm sso Module Components

Introducing the apm sso module ......................................................................... 13-1
Alphabetical list of components .......................................................................... 13-1
basic ....................................................................................................................... 13-2
form-based .......................................................................................................... 13-5
form-basedv2 ......................................................................................................... 13-9
kerberos ............................................................................................................... 13-18
ntlmv1 .................................................................................................................. 13-22
ntlmv2 .................................................................................................................. 13-25

14

asm Module Components

Introducing the asm module .............................................................................. 14-1
Alphabetical list of components .......................................................................... 14-1
device-sync .......................................................................................................... 14-2
httpclass-asm ..................................................................................................... 14-3
predefined-policy ............................................................................................... 14-5
webapp-language ............................................................................................... 14-7

15

auth Module Components

Introducing the auth module ................................................................................ 15-1
Alphabetical list of components .......................................................................... 15-1
cert-ldap .............................................................................................................. 15-2
ldap ....................................................................................................................... 15-8
login-failures ....................................................................................................... 15-13
partition .............................................................................................................. 15-15
password ............................................................................................................. 15-17
### Table of Contents

<table>
<thead>
<tr>
<th>Module</th>
<th>Components</th>
</tr>
</thead>
<tbody>
<tr>
<td>cli</td>
<td>password-policy ................................................................. 15-18</td>
</tr>
<tr>
<td></td>
<td>radius ................................................................. 15-21</td>
</tr>
<tr>
<td></td>
<td>radius-server ............................................................ 15-24</td>
</tr>
<tr>
<td></td>
<td>remote-role ............................................................. 15-27</td>
</tr>
<tr>
<td></td>
<td>remote-user ............................................................. 15-32</td>
</tr>
<tr>
<td></td>
<td>source ................................................................. 15-34</td>
</tr>
<tr>
<td></td>
<td>tacacs ................................................................. 15-36</td>
</tr>
<tr>
<td></td>
<td>user ................................................................. 15-40</td>
</tr>
<tr>
<td></td>
<td>cli alias Module Components</td>
</tr>
<tr>
<td></td>
<td>Introducing the cli alias module .................................................. 17-1</td>
</tr>
<tr>
<td></td>
<td>Alphabetical list of components ................................................. 17-1</td>
</tr>
<tr>
<td></td>
<td>private ................................................................. 17-2</td>
</tr>
<tr>
<td></td>
<td>shared ................................................................. 17-5</td>
</tr>
<tr>
<td></td>
<td>cm Module Components</td>
</tr>
<tr>
<td></td>
<td>Introducing the cm module .................................................. 18-1</td>
</tr>
<tr>
<td></td>
<td>Alphabetical list of components ................................................. 18-1</td>
</tr>
<tr>
<td></td>
<td>cert ................................................................. 18-2</td>
</tr>
<tr>
<td></td>
<td>config-sync .......................................................... 18-6</td>
</tr>
<tr>
<td></td>
<td>device ................................................................. 18-8</td>
</tr>
<tr>
<td></td>
<td>device-group ......................................................... 18-12</td>
</tr>
<tr>
<td></td>
<td>failover-status ...................................................... 18-15</td>
</tr>
<tr>
<td></td>
<td>key ................................................................. 18-16</td>
</tr>
<tr>
<td></td>
<td>sniff-updates ......................................................... 18-19</td>
</tr>
<tr>
<td></td>
<td>sync-status .......................................................... 18-21</td>
</tr>
<tr>
<td></td>
<td>traffic-group ...................................................... 18-22</td>
</tr>
<tr>
<td></td>
<td>trust-domain .......................................................... 18-25</td>
</tr>
<tr>
<td></td>
<td>watch-devicegroup-device ............................................... 18-29</td>
</tr>
<tr>
<td></td>
<td>watch-sys-device .................................................... 18-31</td>
</tr>
<tr>
<td></td>
<td>watch-trafficgroup-device ................................................ 18-33</td>
</tr>
<tr>
<td></td>
<td>gtm Module Components</td>
</tr>
<tr>
<td></td>
<td>Introducing the gtm module .................................................. 19-1</td>
</tr>
<tr>
<td></td>
<td>Alphabetical list of components ................................................. 19-1</td>
</tr>
<tr>
<td></td>
<td>datacenter ........................................................... 19-2</td>
</tr>
<tr>
<td></td>
<td>distributed-app .................................................... 19-5</td>
</tr>
<tr>
<td></td>
<td>iquery ............................................................... 19-9</td>
</tr>
<tr>
<td></td>
<td>ldns ................................................................. 19-10</td>
</tr>
</tbody>
</table>
## Table of Contents

<table>
<thead>
<tr>
<th>Component</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>tcp-half-open</td>
<td>21-11</td>
</tr>
<tr>
<td>tcp</td>
<td>21-108</td>
</tr>
<tr>
<td>soap</td>
<td>21-103</td>
</tr>
<tr>
<td>snmp-link</td>
<td>21-99</td>
</tr>
<tr>
<td>snmp</td>
<td>21-95</td>
</tr>
<tr>
<td>smtp</td>
<td>21-91</td>
</tr>
<tr>
<td>sip</td>
<td>21-86</td>
</tr>
<tr>
<td>scripted</td>
<td>21-82</td>
</tr>
<tr>
<td>real-server</td>
<td>21-79</td>
</tr>
<tr>
<td>radius-accounting</td>
<td>21-75</td>
</tr>
<tr>
<td>real-server</td>
<td>21-79</td>
</tr>
<tr>
<td>scripted</td>
<td>21-82</td>
</tr>
<tr>
<td>sip</td>
<td>21-86</td>
</tr>
<tr>
<td>smtp</td>
<td>21-91</td>
</tr>
<tr>
<td>snmp</td>
<td>21-95</td>
</tr>
<tr>
<td>snmp-link</td>
<td>21-99</td>
</tr>
<tr>
<td>soap</td>
<td>21-103</td>
</tr>
<tr>
<td>tcp</td>
<td>21-108</td>
</tr>
<tr>
<td>tcp-half-open</td>
<td>21-112</td>
</tr>
<tr>
<td>udp</td>
<td>21-116</td>
</tr>
</tbody>
</table>

## 20

gtm global-settings Module Components

Introducing the gtm global-settings module ................................................................. 20-1
Alphabetical list of components ................................................................................. 20-1
general ........................................................................................................................... 20-2
load-balancing .............................................................................................................. 20-6
metrics ........................................................................................................................... 20-8
metrics-exclusions ....................................................................................................... 20-11

## 21

gtm monitor Module Components

Introducing the gtm monitor module ............................................................................. 21-1
Alphabetical list of components .................................................................................. 21-1
bigip .............................................................................................................................. 21-2
bigip-link ..............................................................
external ........................................................................................................................... 21-6
firepass ..............................................................
ftp ................................................................................................................................. 21-13
gateway-icmp ..............................................................
http ............................................................................................................................... 21-21
https ............................................................................................................................. 21-25
imap .............................................................................................................................. 21-34
ldap .............................................................................................................................. 21-38
mssql ............................................................................................................................. 21-43
mysql ............................................................................................................................. 21-48
nntp ............................................................................................................................... 21-53
oracle ..............................................................
pop3 ............................................................................................................................... 21-57
postgresql ..............................................................
radius ..............................................................
radius-accounting ..............................................................
real-server ..............................................................
scripted ..............................................................
sip ................................................................................................................................. 21-62
smtp ............................................................................................................................. 21-66
snmp ............................................................................................................................. 21-71
snmp-link ..............................................................
snmp ..............................................................
snmp ..............................................................
soap ..............................................................
tcp ..............................................................
tcp ..............................................................
tcp-half-open ..............................................................
udp ..............................................................
22

ltm Module Components

Introducing the ltm module ......................................................... 22-1
Alphabetical list of components ............................................... 22-1
default-node-monitor ............................................................... 22-2
ifile ......................................................................................... 22-4
nat .......................................................................................... 22-6
node ....................................................................................... 22-9
pool ....................................................................................... 22-13
rule ....................................................................................... 22-24
snat ....................................................................................... 22-28
snatpool .................................................................................. 22-32
snat-translation ...................................................................... 22-35
tce-policy ............................................................................... 22-38
traffic-class ............................................................................ 22-41
virtual ................................................................................... 22-44
virtual-address ....................................................................... 22-52

23

ltm auth Module Components

Introducing the ltm auth module .................................................. 23-1
Alphabetical list of components ............................................... 23-1
crdp-server ............................................................................. 23-2
kerberos-delegation ............................................................... 23-5
ldap ....................................................................................... 23-8
ocsp-responder ...................................................................... 23-13
profile .................................................................................. 23-18
radius .................................................................................... 23-22
radius-server ......................................................................... 23-25
ssl-cc-ldap .......................................................................... 23-28
ssl-crdp ............................................................................... 23-33
ssl-ocsp ............................................................................... 23-36
tacacs .................................................................................. 23-39

24

ltm classification Module Components

Introducing the ltm classification module .................................... 24-1
Alphabetical list of components ............................................... 24-1
category ............................................................................... 24-2
http-signature ....................................................................... 24-4
key ....................................................................................... 24-7
signature-update-schedule ..................................................... 24-9
update-signatures .................................................................. 24-11

25

ltm data-group Module Components

Introducing the ltm data-group module ....................................... 25-1
Alphabetical list of components ............................................... 25-1
external ............................................................................... 25-2
internal ............................................................................... 25-6
# Table of Contents

## 26
### Ltm Dns Cache Module Components
- Introducing the Ltm Dns Cache module .................................................. 26-1
- Alphabetical list of components .............................................................. 26-1
- Global-Settings ......................................................................................... 26-2
- Resolver .................................................................................................. 26-4
- Transparent ............................................................................................ 26-8
- Validating-Resolver ................................................................................ 26-11

## 27
### Ltm Dns Cache Records Module Components
- Introducing the Ltm Dns Cache Records module ...................................... 27-1
- Alphabetical list of components .............................................................. 27-1
- Key ......................................................................................................... 27-2
- Msg ....................................................................................................... 27-4
- Nameserver ........................................................................................... 27-6
- Rrset .................................................................................................... 27-9

## 28
### Ltm Dns Dns-Express Module Components
- Introducing the Ltm Dns Dns-Express module .......................................... 28-1
- Alphabetical list of components .............................................................. 28-1
- Db ......................................................................................................... 28-2
- Tsig-Key ............................................................................................... 28-3
- Zone ...................................................................................................... 28-5

## 29
### Ltm Dns Dnssec Module Components
- Introducing the Ltm Dns Dnssec module .................................................. 29-1
- Alphabetical list of components .............................................................. 29-1
- Generation ............................................................................................ 29-2
- Key ....................................................................................................... 29-4
- Zone ...................................................................................................... 29-8

## 30
### Ltm Global-Settings Module Components
- Introducing the Ltm Global-Settings module ........................................... 30-1
- Alphabetical list of components .............................................................. 30-1
- Connection ........................................................................................... 30-2
- General ................................................................................................ 30-4
- Traffic-Control ...................................................................................... 30-6

## 31
### Ltm Monitor Module Components
- Introducing the Ltm Monitor module ....................................................... 31-1
- Alphabetical list of components .............................................................. 31-1
- Diameter ............................................................................................... 31-2
- Dns ....................................................................................................... 31-7
- External ............................................................................................... 31-12
- Firepass ............................................................................................... 31-16
- Ftp ....................................................................................................... 31-20
<table>
<thead>
<tr>
<th>Component</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>gateway-icmp</td>
<td>31-24</td>
</tr>
<tr>
<td>http</td>
<td>31-28</td>
</tr>
<tr>
<td>https</td>
<td>31-33</td>
</tr>
<tr>
<td>icmp</td>
<td>31-38</td>
</tr>
<tr>
<td>imap</td>
<td>31-42</td>
</tr>
<tr>
<td>inband</td>
<td>31-46</td>
</tr>
<tr>
<td>ldap</td>
<td>31-49</td>
</tr>
<tr>
<td>module-score</td>
<td>31-54</td>
</tr>
<tr>
<td>mysql</td>
<td>31-58</td>
</tr>
<tr>
<td>mssql</td>
<td>31-63</td>
</tr>
<tr>
<td>nntp</td>
<td>31-68</td>
</tr>
<tr>
<td>oracle</td>
<td>31-72</td>
</tr>
<tr>
<td>pop3</td>
<td>31-77</td>
</tr>
<tr>
<td>postgresql</td>
<td>31-81</td>
</tr>
<tr>
<td>radius</td>
<td>31-86</td>
</tr>
<tr>
<td>radius-accounting</td>
<td>31-90</td>
</tr>
<tr>
<td>real-server</td>
<td>31-94</td>
</tr>
<tr>
<td>rpc</td>
<td>31-97</td>
</tr>
<tr>
<td>sasp</td>
<td>31-101</td>
</tr>
<tr>
<td>scripted</td>
<td>31-104</td>
</tr>
<tr>
<td>sip</td>
<td>31-108</td>
</tr>
<tr>
<td>smb</td>
<td>31-114</td>
</tr>
<tr>
<td>smtp</td>
<td>31-118</td>
</tr>
<tr>
<td>snmp-dca</td>
<td>31-122</td>
</tr>
<tr>
<td>snmp-dca-base</td>
<td>31-126</td>
</tr>
<tr>
<td>soap</td>
<td>31-129</td>
</tr>
<tr>
<td>tcp</td>
<td>31-134</td>
</tr>
<tr>
<td>tcp-echo</td>
<td>31-139</td>
</tr>
<tr>
<td>tcp-half-open</td>
<td>31-143</td>
</tr>
<tr>
<td>udp</td>
<td>31-147</td>
</tr>
<tr>
<td>virtual-location</td>
<td>31-152</td>
</tr>
<tr>
<td>wap</td>
<td>31-156</td>
</tr>
<tr>
<td>wmi</td>
<td>31-161</td>
</tr>
</tbody>
</table>

32

**ltm persistence Module Components**

**Introducing the ltm persistence module** ................................................................. 32-1
**Alphabetical list of components** ................................................................. 32-1
**cookie** .................................................................................................................. 32-2
**dest-addr** ........................................................................................................... 32-6
**global-settings** ................................................................................................. 32-9
**hash** .................................................................................................................... 32-11
**msrdp** .................................................................................................................. 32-15
**persist-records** ............................................................................................... 32-18
**sip** ....................................................................................................................... 32-21
**source-addr** ....................................................................................................... 32-24
**ssl** ....................................................................................................................... 32-28
**universal** ........................................................................................................... 32-31

33

**ltm profile Module Components**

**Introducing the ltm profile module** ................................................................. 33-1
**Alphabetical list of components** ................................................................. 33-1
**analytics** ........................................................................................................... 33-2
Table of Contents

<table>
<thead>
<tr>
<th>Component</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>certificate-authority</td>
<td>33-11</td>
</tr>
<tr>
<td>classification</td>
<td>33-14</td>
</tr>
<tr>
<td>client-ssl</td>
<td>33-16</td>
</tr>
<tr>
<td>diameter</td>
<td>33-24</td>
</tr>
<tr>
<td>dns</td>
<td>33-28</td>
</tr>
<tr>
<td>fasthttp</td>
<td>33-31</td>
</tr>
<tr>
<td>fastl4</td>
<td>33-36</td>
</tr>
<tr>
<td>ftp</td>
<td>33-41</td>
</tr>
<tr>
<td>http</td>
<td>33-44</td>
</tr>
<tr>
<td>httpclass</td>
<td>33-50</td>
</tr>
<tr>
<td>http-compression</td>
<td>33-54</td>
</tr>
<tr>
<td>iiop</td>
<td>33-59</td>
</tr>
<tr>
<td>mbll</td>
<td>33-62</td>
</tr>
<tr>
<td>ntlm</td>
<td>33-65</td>
</tr>
<tr>
<td>one-connect</td>
<td>33-68</td>
</tr>
<tr>
<td>radius</td>
<td>33-71</td>
</tr>
<tr>
<td>ramcache</td>
<td>33-74</td>
</tr>
<tr>
<td>request-log</td>
<td>33-76</td>
</tr>
<tr>
<td>rtsp</td>
<td>33-80</td>
</tr>
<tr>
<td>sctp</td>
<td>33-84</td>
</tr>
<tr>
<td>server-ssl</td>
<td>33-88</td>
</tr>
<tr>
<td>sip</td>
<td>33-96</td>
</tr>
<tr>
<td>smtp</td>
<td>33-99</td>
</tr>
<tr>
<td>spdy</td>
<td>33-101</td>
</tr>
<tr>
<td>statistics</td>
<td>33-104</td>
</tr>
<tr>
<td>stream</td>
<td>33-108</td>
</tr>
<tr>
<td>tce</td>
<td>33-111</td>
</tr>
<tr>
<td>tcp</td>
<td>33-113</td>
</tr>
<tr>
<td>udp</td>
<td>33-120</td>
</tr>
<tr>
<td>wa-cache</td>
<td>33-123</td>
</tr>
<tr>
<td>xml</td>
<td>33-125</td>
</tr>
</tbody>
</table>

34
ltm tce Module Components

- Introducing the ltm tce module ................................................................. 34-1
- Alphabetical list of components ............................................................... 34-1
- policy ......................................................................................................... 34-2
- steering-endpoint ...................................................................................... 34-5

35
net Module Components

- Introducing the net module ........................................................................... 35-1
- Alphabetical list of components ............................................................... 35-1
- arp .............................................................................................................. 35-2
- cmetrics ................................................................................................... 35-5
-fdb .............................................................................................................. 35-7
- interface .................................................................................................. 35-10
- ndp ............................................................................................................ 35-15
- packet-filter ......................................................................................... 35-17
- packet-filter-trusted ............................................................................... 35-22
- port-mirror ............................................................................................ 35-25
- route ........................................................................................................ 35-27
- route-domain ........................................................................................... 35-30
- router-advertisement ............................................................................... 35-33
## Table of Contents

<table>
<thead>
<tr>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>rst-cause</td>
</tr>
<tr>
<td>self</td>
</tr>
<tr>
<td>self-allow</td>
</tr>
<tr>
<td>stp</td>
</tr>
<tr>
<td>stp-globals</td>
</tr>
<tr>
<td>trunk</td>
</tr>
<tr>
<td>vlan</td>
</tr>
<tr>
<td>vlan-allowed</td>
</tr>
<tr>
<td>vlan-group</td>
</tr>
<tr>
<td>wccp</td>
</tr>
</tbody>
</table>

### 36

**net ipsec Module Components**

- Introducing the net ipsec module: 36-1
- Alphabetical list of components: 36-1
- ike-daemon: 36-2
- ike-peer: 36-4
- ipsec-policy: 36-9
- manual-security-association: 36-12
- traffic-selector: 36-15

### 37

**net rate-shaping Module Components**

- Introducing the net rate-shaping module: 37-1
- Alphabetical list of components: 37-1
- class: 37-2
- drop-policy: 37-7
- queue: 37-11
- shaping-policy: 37-14

### 38

**net tunnels Module Components**

- Introducing the net tunnels module: 38-1
- Alphabetical list of components: 38-1
- etherip: 38-2
- gre: 38-5
- ipip: 38-8
- ppp: 38-11
- tunnel: 38-14
- wccp: 38-17

### 39

**sys Module Components**

- Introducing the sys module: 39-1
- Alphabetical list of components: 39-1
- clock: 39-2
- cluster: 39-3
- config: 39-6
- config-diff: 39-12
- connection: 39-13
- console: 39-16
- cpu: 39-18
- daemon-ha: 39-19
41
sys crypto Module Components
Introducing the sys crypto module ................................................................. 41-1
Alphabetical list of components ................................................................. 41-1
cert .............................................................. 41-2
check-cert ......................................................... 41-5
crl .............................................................. 41-7
key .............................................................. 41-9
master-key ...................................................... 41-13
pkcs12 .......................................................... 41-15

42
sys crypto fips Module Components
Introducing the sys crypto fips module .......................................................... 42-1
Alphabetical list of components ................................................................. 42-1
by-handle ......................................................... 42-2
private-key ...................................................... 42-3
public-key ....................................................... 42-5

43
sys daemon-log-settings Module Components
Introducing the sys daemon-log-settings module ........................................ 43-1
Alphabetical list of components ................................................................. 43-1
clusterd .......................................................... 43-2
csyncd ........................................................... 43-4
lind ............................................................... 43-6
mcpd ............................................................. 43-8
tmm ............................................................... 43-10

44
sys disk Module Components
Introducing the sys disk module ................................................................. 44-1
Alphabetical list of components ................................................................. 44-1
application-volume ................................................................. 44-2
logical-disk ....................................................... 44-4

45
sys file Module Components
Introducing the sys file module ................................................................. 45-1
Alphabetical list of components ................................................................. 45-1
apache-ssl-cert .................................................. 45-2
data-group ....................................................... 45-5
external-monitor ..................................................... 45-8
ssl-cert .......................................................... 45-11
ssl-crl ........................................................... 45-14
ssl-key ........................................................... 45-16

46
sys performance Module Components
Introducing the sys performance module .................................................... 46-1
Alphabetical list of components ................................................................. 46-1
Table of Contents

47
sys raid Module Components
Introducing the sys raid module ................................................................. 47-1
Alphabetical list of components ................................................................. 47-1
array ........................................................................................................... 47-2
bay .............................................................................................................. 47-4
disk .......................................................................................................... 47-6

48
sys software Module Components
Introducing the sys software module .......................................................... 48-1
Alphabetical list of components ................................................................. 48-1
hotfix ......................................................................................................... 48-2
image ........................................................................................................ 48-5
status ...................................................................................................... 48-8
volume .................................................................................................... 48-10

49
util Module Components
Introducing the util module ..................................................................... 49-1
Alphabetical list of components ................................................................. 49-1
test-monitor ......................................................................................... 49-2
tracepath .............................................................................................. 49-3
tracepath6 ........................................................................................... 49-4
ttraceroute ............................................................................................ 49-5
ttracerout6 .......................................................................................... 49-6
vconsole ............................................................................................... 49-7
zebos ..................................................................................................... 49-8

50
vcmp Module Components
Introducing the vcmp module ................................................................. 50-1
Alphabetical list of components .............................................................. 50-1
global ...................................................................................................... 50-2
guest ....................................................................................................... 50-3
vdisk ........................................................................................................ 50-7

51
wam Module Components
Introducing the wam module ................................................................. 51-1
Alphabetical list of components .............................................................. 51-1
application ............................................................................................ 51-2
normalization ....................................................................................... 51-7
object-type ......................................................................................... 51-10
## Table of Contents

- **policy** ................................................................................................................................. 51-13

### 52 wom Module Components

- Introducing the wom module ................................................................................................. 52-1
- Alphabetical list of components .............................................................................................. 52-1
- advertised-route ...................................................................................................................... 52-2
- deduplication ........................................................................................................................... 52-5
- diagnose-conn ......................................................................................................................... 52-7
- endpoint-discovery .................................................................................................................. 52-8
- local-endpoint ......................................................................................................................... 52-11
- remote-endpoint ...................................................................................................................... 52-14
- remote-route ........................................................................................................................... 52-18
- server-discovery ....................................................................................................................... 52-19
- verify-config ............................................................................................................................ 52-23

### 53 wom profile Module Components

- Introducing the wom profile module ...................................................................................... 53-1
- Alphabetical list of components .............................................................................................. 53-1
- cifs ............................................................................................................................................ 53-2
- isession ..................................................................................................................................... 53-5
- mapi .......................................................................................................................................... 53-9

**Glossary**

**Index**
Table of Contents
Introducing the Traffic Management Shell

- About the Traffic Management Shell
- Additional command line utilities and tools
- Basic syntax conventions
About the Traffic Management Shell

The BIG-IP® system includes a tool known as the Traffic Management Shell (tmsh) that you can use to configure and manage the system from the command line. Using tmsh, you can configure system features, and set up network elements. You can also configure the BIG-IP system to manage local and global traffic passing through the system, and view statistics and system performance data.

You can use tmsh in conjunction with the Configuration utility, which is the browser-based BIG-IP system and network management tool.

All products in the BIG-IP product family run on the powerful Traffic Management Operating System®, commonly referred to as TMOS®. For an overview of the complete BIG-IP product offering, see the TMOS® Management Guide for BIG-IP® Systems.
Additional command line utilities and tools

There are several additional command line utilities and tools that you can use to configure and manage the BIG-IP system:

- **The config utility**
  You use the `config` utility to define the IP address, network mask, and gateway for the management (MGMT) port, when you initially set up the BIG-IP system.

- **The bigtop utility**
  The `bigtop` utility is a statistical monitoring utility that ships on the BIG-IP system. This utility provides real-time statistical information. You can set a refresh interval and specify a sort order for this statistical information.

- **The bigstart command**
  With the `bigstart` command, you can start, stop, restart, and check the status of various daemons, such as `snmpd`.

- **The gencert utility**
  You can use the `gencert` utility to generate a key, a temporary certificate and a certificate signing request file. You then submit the request file to a certificate authority to obtain an SSL certificate.

The industry-standard tools that you can also use to manage the BIG-IP system are:

- **The Tools Command Language (Tcl) programming language**
  The Tools Command Language (Tcl) programming language is an industry-standard programming language that you can use to create BIG-IP system iRules®. iRules are scripts you can write to direct and manipulate the way that the BIG-IP system manages application traffic.

- **The OpenSSL utility**
  A component of the industry-standard OpenSSL toolkit, the OpenSSL utility is a set of commands that perform various cryptographic functions, such as generating SSL certificates and keys.
**Basic syntax conventions**

The following table lists basic syntax conventions that apply throughout this guide.

<table>
<thead>
<tr>
<th>Item in text</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>()</td>
<td>Specifies that the syntax inside the parentheses is optional.</td>
</tr>
<tr>
<td>...</td>
<td>Specifies that you can type a series of items.</td>
</tr>
<tr>
<td>[ ]</td>
<td>Identifies a user-defined parameter in <code>tmsh</code>. For example, if the syntax shows <code>[your name]</code>, type in your name, but do not include the brackets.</td>
</tr>
<tr>
<td></td>
<td>Specifies a choice between options.</td>
</tr>
<tr>
<td>[integer]</td>
<td>Specifies a numeric attribute. Unless there is a system assigned default value, the default value is 0 (zero).</td>
</tr>
<tr>
<td>[ip address]</td>
<td>Specifies an IPv4 or IPv6 address.</td>
</tr>
<tr>
<td>[mac-address]</td>
<td>Specifies six hexadecimal numbers separated by colons.</td>
</tr>
</tbody>
</table>

*Table 1.1  Command line syntax conventions*
Chapter 1
Understanding and Using the Traffic Management Shell

- Understanding the structure of tmsh
- Using tmsh
- Introduction to command syntax
Understanding the structure of tmsh

**tmsh** is an interactive shell that you use to manage the BIG-IP® system. The structure of **tmsh** is hierarchical and modular. The highest level is the **root** module, which contains twelve subordinate modules.

Several modules also contain subordinate modules. All modules and subordinate modules contain components that you configure to manage the BIG-IP system. You can configure a component that resides anywhere in the hierarchy from anywhere else in the hierarchy by using the full path to that component. Alternatively, you can configure a component by navigating to that component directly. After you create a component, you can modify that component in object mode, which is the lowest level of the hierarchy.

![Figure 2.1 The tmsh modular structure](image)

*Figure 2.1 The tmsh modular structure*
Using tmsh

You must provision a BIG-IP module before you can use tmsh to configure it. The command sequence list sys provision displays the BIG-IP system modules that can be provisioned.

**Important**

*tmsh* applies all configuration changes that you make from within *tmsh* to the running configuration of the system. For *tmsh* to write the changes to the stored configuration files, you must save the changes using the save sys config command sequence.

You can run *tmsh* and issue commands in the following ways:

- You can issue a single *tmsh* command at the BIG-IP system prompt using this syntax:

  ```
  tmsh [command] [module...module] [component] (options)
  ```

  For example, you can display all the properties of all BIG-IP system pools by typing the following command sequence at the BIG-IP system prompt:

  ```
  tmsh show ltm pool all-properties
  ```

- You can open *tmsh* by typing *tmsh* at the BIG-IP system prompt. This starts *tmsh* in interactive shell mode and displays the *tmsh* prompt: *(tmos)#.*

Loading and saving the system configuration

The system applies all configuration changes that you make from within *tmsh* to the running configuration of the system. You can save a portion of the running configuration known as the base configuration. You can also load the base configuration from the stored configuration files.

- To save the base configuration to the stored configuration files, use the following command sequence:

  ```
  save /sys base-config
  ```

- To replace the base configuration with the configuration in the stored configuration files, use the following command sequence:

  ```
  load /sys base-config
  ```

- To save the entire running configuration to the stored configuration files, use the following command sequence:

  ```
  save /sys config
  ```

- To replace the entire running configuration with the configuration in the stored configuration files using the following command sequence:

  ```
  load /sys config
  ```
Working within the tmsh hierarchy

It is important to understand how to use the command syntax based on where you are in the tmsh hierarchy.

When you are working in the root module, you enter a command sequence using this syntax:

```
[command] [module...module] [component] (options)
```

When you are working in a subordinate module, and you want to configure a component that resides within another module, you enter a command sequence using this syntax:

```
[command] / [module...module] [component] (options)
```

Note that the slash provides the path from one module to another.

As you navigate within tmsh, the prompt contains a visual cue to your location within the hierarchy.

You can navigate to a module, a component within a module, or a specific component (object mode). The following list provides examples of how the tmsh prompt changes as you navigate through the hierarchy. From the root module prompt:

- To navigate to the ltm module, type: `ltm`
  The ltm module prompt displays: `(tmos.ltm)#`
- To navigate to the ltm pool component, type: `ltm pool`
  The ltm pool component prompt displays: `(tmos.ltm.pool)#`
- To navigate to `pool1`, type: `modify ltm pool pool1`
  The pool1 object prompt displays: `(tmos.ltm.pool.pool1)#`

**Note**

You can navigate only to an object that already exists, and you must use the modify command to navigate to that object.

**Tip**

You can change the information that displays in the tmsh prompt, but the prompt always includes your location in the hierarchy and ends with a pound sign (#). For information about customizing the prompt, see preference, on page 16-8.

Working within a module

From the root module, you can navigate to another module by entering the name of the module at the prompt. tmsh opens the module, and displays the prompt: `(tmos.module)#`

For example, from the root module, to navigate to the gtm module, type:

`gtm`

The prompt now indicates that the current location in the hierarchy is the gtm module.
Within a module, you can type a command sequence using this syntax:

\[
\text{[command]} \ [\text{component}] \ (\text{options})
\]

For example, you can display all the properties of all Global Traffic Manager™ pools by entering the following command sequence at the `gtm` module prompt:

\[
\text{list pool all-properties}
\]

Additionally, from a module, you can manage a component in a different module using this syntax:

\[
\text{[command]} / / [\text{module...module}] \ [\text{component}] \ (\text{options})
\]

For example, from the `gtm` module, you can show all of the properties of the VLANs on your network by entering the following command sequence at the `gtm` module prompt:

\[
\text{list / net vlan all-properties}
\]

### Working within a component

From a `tmsh` module, you can navigate to a component by entering the name of the component at the prompt. `tmsh` displays the component prompt:

\[
(tmos.module.component)#
\]

For example, from the `gtm` module, to navigate to the `gtm pool` module, type:

\[
\text{pool}
\]

The prompt now indicates that the current location in the hierarchy is the `gtm pool` component.

Within the component, you can type a command sequence using this syntax:

\[
\text{[command]} \ (\text{options})
\]

For example, you can display all of the properties of all of the Local Traffic Manager™ pools by entering the following command sequence at the `ltm pool` component prompt:

\[
\text{list all-properties}
\]

From within a component, you can also manage a component in a different module using this syntax:

\[
\text{[command]} / / [\text{module...module}] \ [\text{component}] \ (\text{options})
\]

Note that you can manage a component from anywhere within the `tmsh` hierarchy by using the full path to the component.

For example, from the `gtm pool` component, you can show all of the properties of the VLANs on your network by entering the following command sequence at the prompt:

\[
\text{list / net vlan all-properties}
\]
Working in object mode

From a tmsh component, you can navigate to a specific object of that type, by entering the modify command followed by the name of the component at the prompt. tmsh opens the component and displays the prompt:

(tmos.module.component.object_name)#

For example, from the gtm pool module, to navigate to the Global Traffic Manager pool, named pool1, type:

modify pool1

The prompt now indicates that the current location in the hierarchy is the gtm pool pool1 object.

The Properties list contains the available properties of the current object.

For example, to navigate to the Global Traffic Manager pool named pool1 type the following command sequence:

modify gtm pool pool1

tmsh displays this prompt: (tmos.gtm.pool.pool1)#

In the object mode, you can type a command sequence using this syntax:

[command] (options)

For example, you can display all of the properties of gtm pool by entering the following command sequence at the gtm pool1 object prompt:

list all-properties

From within an object, you can also manage a component in a different module using this syntax:

[command] / [module...module] [component] (options)

For example, from within the gtm pool pool1 object, you can display all of the properties of the Local Traffic Manager™ pool named my_pool by entering the following command sequence at the gtm pool pool1 object prompt:

list / ltm pool pool1 all-properties
Leaving object mode, component mode, a module, or tmsh

Table 2.1 describes the commands you use to navigate out of a mode or a module, and eventually close tmsh and return to the BIG-IP system prompt.

<table>
<thead>
<tr>
<th>Command</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>/</td>
<td>From any level of the tmsh hierarchy, returns you to the root module.</td>
</tr>
<tr>
<td>exit</td>
<td>From within object mode, returns you to the component within which the object resides. From within a component, returns you to the module within which the component resides. From within a module, returns you to the parent module.</td>
</tr>
<tr>
<td>quit</td>
<td>From within a module, closes tmsh.</td>
</tr>
</tbody>
</table>

Table 2.1 Commands for navigating out of a mode or module, and for closing tmsh

Using the scripting feature

You can use the tmsh script component to build Tcl scripts to automate and customize management of the BIG-IP system. The tmsh scripting feature is a small API that provides structured programmatic access to all system configuration, status, and statistics. The API mirrors the interactive command line syntax. The structured access of the API eliminates the need to screen scrape output.

Using the tmsh scripting feature, you can write scripts that perform the following:

- Accept parameters from the command line
- Provide command completion and context-sensitive help
- Handle the management of complex system configurations with simple form-based input
- Run in their own execution environment separate from the shell from which they were started

This feature also gives you the ability to perform the following:

- Build reusable script libraries and include them in other scripts using the #include directive
- Use transactional semantics
- Combine command aliases with scripts, allowing you to extend tmsh to build commands that are customized to your environment

For more information about the tmsh script component, see script, on page 16-14.
Understanding and Using the Traffic Management Shell

Using the command completion feature

At any point while typing or editing a command in tmsh, you can press the Tab key. tmsh either completes the current or next word, or displays possible completions for the current or next word.

The command completion feature reduces the amount of typing that is required to run commands. When you press the Tab key, the system automatically completes the current command-line element to as many unique characters as possible. If there is more than one possible completion the list of possible completions displays. Command completion also completes configuration object identifiers.

For example, if the command has only one option, tmsh fills in the remainder of the word with that option and a trailing space. If the command has more than one option, tmsh completes the current word with the longest possible match, while also displaying the other possible matches. If tmsh displays nothing after you press the Tab key, no options exist to complete the word.

If you move the cursor anywhere on the command line and press the Tab key, tmsh completes what is to the left of the cursor. For example, tmsh completes sho[Tab] pool as show pool.

Using glob matching with the command completion feature

tmsh uses glob matching to complete object identifiers. glob matching checks for the presence of the constituents of a given pattern. This means that if you partially type an object identifier, such as the IP address of a node, tmsh completes the command by offering all IP addresses that contain the partial address you entered.

For example, tmsh returns addresses that match 10.1.1* when you type the following command sequence:

```
show node 10.1.1[Tab]
```

Likewise, tmsh returns addresses that match 10*22*, when you type the following command sequence:

```
show node 10*22[Tab]
```

Understanding the behavior of the command completion feature

There are several behaviors to be aware of when using the command completion feature. When you press the Tab key, the components that display in the Configuration Items list are determined by your permissions and the action you are taking. The following rules apply:

- When you configure a component that is not a child component, the Configuration Items list contains the existing components of the type that you are configuring that you have permission to view.

For example, tmsh displays all virtual servers that you have permission to view in the Configuration Items list when you configure a virtual server using the following syntax:

```
[create | delete | modify] virtual [Tab]
```
When you configure a child component, (for example, when you add a pool member to a pool), the Configuration Items list contains the existing components of the type that you are configuring based on the following rules:

- When you add a child component to its parent, the list contains only the components of that type that you have permission to view that are not yet associated with the parent component. For example, the list contains all of the virtual servers that you have permission to view that are not yet associated with poolA when you add members to poolA using the following syntax:

  ```
  modify pool poolA members add {}
  ```

- When you replace all of the child components that are associated with a parent component, the list contains all of the components of that type that you have permission to view. For example, the list contains all of the virtual servers that you have permission to view when you replace all of the members of poolA using the following syntax:

  ```
  modify pool poolA members replace-all-with {}
  ```

- When you delete or modify the child components that are associated with a parent component, the list contains only the components of that type that are already associated with the parent. For example, the list contains all of the virtual servers that are currently a member of poolA when you delete the members of poolA using the following syntax:

  ```
  modify pool poolA members delete {}
  ```

- When you configure a component, the Properties list only contains properties that you can use with other already configured properties of that component.

  The command route is a good example. If you specify a pool for the route, then the interface, gateway, and blackhole options are no longer valid, so they do not appear in the list.

**Tip**

At the BIG-IP system prompt, tmsh displays possible completions for a command, only if you type the tmsh command followed by:

\[ Ctrl + V Ctrl + T Enter \]

**Using the help feature**

tmsh includes man pages for each of the commands and components that are available within tmsh. You access the man pages using the following command syntax:

```
help [ [command] | [full path to component] ]
```

For example, to access the man page for the vlan component from the root module, use the following command sequence:

```
help / net vlancl
```
You can also search the man pages for information on a specific term or topic. To do this, you use the following command syntax:

```
help search [term or topic]
```

You can perform a help search from within any module in the `tmsh` hierarchy. For example, to find the man pages that contain a reference to VLANs, use the following command sequence:

```
help search vlan
```

Additionally, you can display a list of topics that are available in a module using the following command sequence:

```
help [full path to module]
```

For example, to display the topics that are available in the current module, use this command: `help`. To display the topics that are available in the `net` module, use the following command sequence: `help / net`.

### Using the context-sensitive help feature

`tmsh` includes a context-sensitive help feature that provides help as you type commands. At any time, you can type a question mark (`?`) on the command line, and `tmsh` returns information to assist you in completing the command. Based on when you type the question mark, you get the following results:

- When you type a question mark immediately following any portion of a command, `tmsh` returns possible completions for the command, but does not complete the command as the command completion feature does.
- When you type a space before the question mark, `tmsh` returns descriptive text that explains the commands, components, or properties that you can configure.
- When you type a question mark in the middle of a command, `tmsh` returns help on the command to the left of the cursor.

**Note**

To use a question mark in a `glob` or regular expression, you must escape the question mark using quotation marks, apostrophes, or a backslash.

Additionally, you can request context-sensitive help for the last command in a series of commands. For more information, see *Entering multiple commands*.

### Interrupting a command

You can cancel a command that you issued by typing `Ctrl + C` one or more times.
Entering multiple commands

You can enter multiple commands on the command line by separating the commands with semi-colons (;). For example, to display the properties of the self IP addresses and VLANs of the system, use the following command sequence:

```
list / net self ; list / net vlan
```

When you enter multiple commands in this way, all of the commands are added to the command glob in a single line item, regardless of whether any of the commands were successful. However, if one of the commands that you enter fails to parse, tmsh does not run the remaining commands you entered. tmsh audits commands as the commands run; therefore, if a command fails to parse, tmsh does not audit the remaining commands.

You can also specify multiple commands in a command alias by separating the commands with semi-colons. For example, to create an alias that displays the properties of the VLANs and VLAN groups on the system, use the following command sequence:

```
create / cli alias vlans command "list / net vlan ; list / net vlan-group"
```

Additionally, you can request context-sensitive help and use the command completion feature on the last command in a series of commands. For example, to display help for the vlan-group component, use the following command sequence:

```
list / net vlan ; list / net vlan-group ?
```

Using the command glob feature

tmsh saves each command that you enter in the command glob file. The date and time the command was issued displays before the command in this format: [Month day hh:mm:ss]. You can disable this feature.

To change whether the date and time display in the glob file

1. Log on to tmsh and navigate to the cli preference module.
2. To disable the display of the date and time in the glob file, type: `modify glob-date-time disabled`
3. To enable the display of the date and time in the glob file, type: `modify glob-date-time enabled`

The command glob persists when you log off of the system. The next time you log on to the system, you can search for, display, and then edit, the tmsh commands that you entered in previous sessions. The command glob persists even through a restart of the BIG-IP system.
There are two limits that you can set for the command glob: the number of commands that tmsh saves in the command glob file, and the number of commands that you can view or search from the command line.

- You use the set cli preference glob-file-size command to set the maximum number of commands that you want tmsh to save in the command glob file.
  
  The default is 10,000 commands. The maximum number of commands that the file can contain is 100,000 commands. If you do not want to use the command glob feature, set the maximum number of commands to 0 (zero). This means that tmsh does not save any commands in the glob file.

- You use the set cli preference glob-size command to set the number of commands that you want to be able to view or search from the command line.
  
  The default is 500 commands. The maximum number of commands that you can view or search is 10,000 commands. When you set the glob-size option to (0) zero, tmsh does not add commands to the in-memory list of commands, but does continue to write commands to the command glob file.

  Note: After you change the value of the glob-size option, tmsh might renumber the commands; however, the commands remain in the same order.

- Tip

  tmsh does not save commands in the command glob file that end in a question mark (?) or begin with an exclamation point (!). Likewise, these types of commands do not appear in the command glob list.

To display the commands in the tmsh glob list

1. Log on to tmsh.
2. Enter an exclamation point (!).
   
   The command glob list displays the previously used commands in the reverse order of use.
3. After you locate the command that you want to use again, type:

   ! [numeric ID]

   For example, to run the command with a numeric ID of 32, type:

   !32

- Note

  Each command in the glob list is identified by a numeric ID. The larger the ID, the more recently the command was issued relative to other commands.
To search for and run a command in the `tmsh glob` list using a partial string

1. Log on to `tmsh`. The `tmsh` prompt displays.
2. To run the most recent command in the `glob` list that begins with the specified string, type the following command:

   `! [string]`

   `tmsh` locates the command in the `glob` list and runs it.

   For example, from the `cli` module, to run the most recent command that you used to set the preferences for the command line, type:

   `! set preference`.

When you are logged on to `tmsh`, you can use the `glob` list to run the previous command, even if it was run in the previous `tmsh` session.

To run the previous command

1. Issue commands to configure the system.

   `tmsh` runs the commands you issue.

2. Type the following command:

   `!!`

   The previous command runs.

When you are logged on to `tmsh`, you can use pager’s search feature to locate a `tmsh` command by date/time stamp.

To search for a command using the pager’s search feature

1. Log on to `tmsh`.
2. Type one of the following commands:

   `show glob`

   or

   `!`

3. Use the pager’s search feature to find a specific date and time.

When you are logged on to `tmsh`, you can pipe the output of the `glob` file to the `grep` utility to search for a command by the date/time stamp.

To search for a command using the `grep` utility

1. Log on to `tmsh`.
2. Type the following command:

   `show glob | grep "[hh:mm:ss]"`
Using the tmsh keyboard map feature

You can use the default keyboard map to search the command glob list for a specified command. For example, to search for the previous command that contains a specified string, type the following command:

```
[string] Alt-P
```

You must press Enter to run the command.

The following table describes the default keyboard map for tmsh. The key sequences are not case-sensitive.

<table>
<thead>
<tr>
<th>Key Sequence</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ctrl + A</td>
<td>Moves the cursor to the beginning of the line.</td>
</tr>
<tr>
<td>Ctrl + B</td>
<td>Moves the cursor to the left one character.</td>
</tr>
<tr>
<td>Ctrl + C</td>
<td>Cancels the current command.</td>
</tr>
<tr>
<td>Ctrl + D</td>
<td>Deletes the character under the cursor, or when the command line is empty, exits tmsh.</td>
</tr>
<tr>
<td>Ctrl + E</td>
<td>Moves the cursor to the end of the line.</td>
</tr>
<tr>
<td>Ctrl + F</td>
<td>Moves the cursor to the right one character.</td>
</tr>
<tr>
<td>Ctrl + G</td>
<td>Clears all characters from the command line.</td>
</tr>
<tr>
<td>Ctrl + H</td>
<td>Deletes the previous character.</td>
</tr>
<tr>
<td>Ctrl + J</td>
<td>Enters a new line and runs the current command.</td>
</tr>
<tr>
<td>Ctrl + K</td>
<td>Deletes all characters from the cursor to the end of the line.</td>
</tr>
<tr>
<td>Ctrl + L</td>
<td>Clears the screen, repositions the prompt at the upper left, and leaves the current command intact.</td>
</tr>
<tr>
<td>Ctrl + M</td>
<td>Enters a new line and runs the current command.</td>
</tr>
<tr>
<td>Ctrl + N</td>
<td>Displays the next item in the command glob.</td>
</tr>
<tr>
<td>Ctrl + P</td>
<td>Displays the previous item in the command glob.</td>
</tr>
<tr>
<td>Ctrl + Q</td>
<td>Resumes input.</td>
</tr>
<tr>
<td>Ctrl + R</td>
<td>Clears the screen, repositions the prompt at upper left, and leaves the current command intact.</td>
</tr>
<tr>
<td>Ctrl + S</td>
<td>Suspends input.</td>
</tr>
<tr>
<td>Ctrl + T</td>
<td>Transposes the character under the cursor with the character to the left of the cursor.</td>
</tr>
<tr>
<td>Ctrl + U</td>
<td>Deletes all characters before the cursor.</td>
</tr>
</tbody>
</table>

*Table 2.2 Default keyboard map for tmsh*
Using the command audit feature

The BIG-IP system contains a read-only audit file named /var/log/audit. `tmsh` writes an entry in the audit file for each `tmsh` command that runs, providing a historical log of issued commands. Only users with the role of Administrator or Resource-Administrator can view the audit logs.

You can change whether `tmsh` audits commands using the following syntax:
```
modify / cli global-settings audit [enabled | disabled]
```

<table>
<thead>
<tr>
<th>Key Sequence</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ctrl + W</td>
<td>Deletes the word before the cursor.</td>
</tr>
<tr>
<td>Esc + B</td>
<td>Moves the cursor one word to the left.</td>
</tr>
<tr>
<td>Esc + D</td>
<td>Deletes all characters from the cursor to the end of the current or next word.</td>
</tr>
<tr>
<td>Esc + F</td>
<td>Moves the cursor one word to the right.</td>
</tr>
<tr>
<td>Esc + L</td>
<td>Changes the word to the right and the word under the cursor to lowercase.</td>
</tr>
<tr>
<td>Esc + N</td>
<td>Searches command <code>glob</code> search for the next item.</td>
</tr>
<tr>
<td>Esc + P</td>
<td>Searches command <code>glob</code> search for the previous item.</td>
</tr>
<tr>
<td>Esc + U</td>
<td>Changes the word to the right and the word under the cursor to uppercase.</td>
</tr>
<tr>
<td>Esc + Backspace</td>
<td>Deletes the word to the left of the cursor.</td>
</tr>
<tr>
<td>Backspace</td>
<td>Deletes the character to the left of the cursor.</td>
</tr>
<tr>
<td>Delete</td>
<td>Deletes the character to the left of the cursor.</td>
</tr>
<tr>
<td>Up Arrow</td>
<td>Scrolls back through the command <code>glob</code>.</td>
</tr>
<tr>
<td>Down Arrow</td>
<td>Scrolls forward through the command <code>glob</code>.</td>
</tr>
</tbody>
</table>

*Table 2.2 Default keyboard map for tmsh (Continued)*

◆ **Note**

*If tmsh cannot connect to the mcpd daemon, tmsh audits all commands until the connection is re-established.*
Understanding the audit log entries

The audit file contains entries with the format shown in Figure 2.2.

01420002:5: AUDIT – pid=number user=user_id query_partitions=p1,p2,...,pn
update_partition=partition_name module=(tmos.module...)# status=[success/fail]
cmd_data=command that was issued

Figure 2.2 Audit file entry format

Table 2.3 defines each portion of an audit entry in the order of appearance in the entry.

<table>
<thead>
<tr>
<th>Audit Entry</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>01420002:5: AUDIT</td>
<td>Identifies the entry as a tmsh command.</td>
</tr>
<tr>
<td>pid=number</td>
<td>Specifies the process ID of the tmsh instance that generated the entry.</td>
</tr>
<tr>
<td>user=user_id</td>
<td>Identifies, by user ID, the user who issued the tmsh command. For commands run by the system, this portion of the entry is empty, for example: user=“ “.</td>
</tr>
<tr>
<td>query_partitions=</td>
<td>Identifies the administrative partitions, in a comma-separated list, that the user can query. For more information about setting the administrative partitions, see admin-partitions, on page 16-2.</td>
</tr>
<tr>
<td>update_partition=</td>
<td>Identifies the administrative partitions that the user can update. For more information about setting the administrative partitions that a user can update, see admin-partitions, on page 16-2.</td>
</tr>
<tr>
<td>module=</td>
<td>Identifies the tmsh module within which the user issued the command.</td>
</tr>
<tr>
<td>status</td>
<td>Indicates whether the command was run successfully. The possible values are:</td>
</tr>
<tr>
<td></td>
<td>• Command OK</td>
</tr>
<tr>
<td></td>
<td>• [error syntax]</td>
</tr>
<tr>
<td>cmd_data=</td>
<td>Indicates the command sequence that the user entered. Note that when the edit command runs successfully, the audit file contains each line of the file that was submitted as a separate entry. For more information about the command edit, see rule, on page 19-41.</td>
</tr>
</tbody>
</table>

Table 2.3 Audit entries defined
Chapter 2

Viewing historical logs

When you view an audit log from \texttt{tmsh}, you can use the \texttt{lines} or \texttt{range} options to reduce the number of log entries that display. For more information about these options, see \texttt{log}, on page 39-60.

\textbf{To view historical logs}

1. Log on to \texttt{tmsh}.
   The \texttt{tmsh} prompt displays.

2. Type the following command sequence:
   \texttt{show / sys log audit lines 5}
   The first five lines in the audit log display.

Using the command aliases feature

You can create command aliases to use as short cuts within \texttt{tmsh}. For example, if you perform specific operations on a regular basis, or if you configure the system using long commands, you can create a command alias to save you some typing.

You can issue a command alias from within any \texttt{tmsh} module. For example, if you create an alias named \texttt{show} to display all of the components in the \texttt{ltm} module, when you type \texttt{show} in the \texttt{cli} module, \texttt{tmsh} displays only the \texttt{ltm} module components. This example illustrates that the command alias you created takes precedence over the system default \texttt{show} command, which normally displays the components of the module within which you issue the command.

\textbf{WARNING}

\texttt{Aliases that you create take precedence over system commands. Additionally, an alias with the same name as a \texttt{tmsh} module causes the module to be hidden from the command completion feature.}

Creating command aliases

A command alias consists of a name and a command sequence that runs when you use the name of the command alias on the command line. When you create a command alias, the name of the command alias:

\begin{itemize}
  \item Is not case-sensitive
  \item Cannot be \texttt{create} or \texttt{delete}
  \item Cannot contain spaces, tabs, exclamation points, or question marks
\end{itemize}

The following rules apply to the command sequence for which you are creating a command alias.

\begin{itemize}
  \item The command cannot be empty.
  \item You can use multiple command sequences, separated by semi-colons.
\end{itemize}
• You can use another alias as the first argument in the command sequence.
• `tmsh` does not verify validity of the command sequence until you issue the command alias.
• When you include an exclamation point in the command sequence, the exclamation point does not invoke the command `glob`.
• If you include spaces in the command sequence, then you must use quotation marks around the command sequence.

Using command aliases

When you use a command alias on the command line, the following rules apply:
• When you use a command alias within a command, you must use the alias at the beginning of the command sequence.
• When you use the command completion or context-sensitive help feature with a command alias, `tmsh` responds as if you had entered the command sequence that the command alias references.
• Command aliases display in all command completion lists, regardless of whether the command itself is valid within the current module.
• The name of the command alias displays in the command `glob` list.
• The command, for which you created the alias, not the name of the command alias, displays in error messages related to usage of the alias.

Setting the tmsh preference show-aliases

You can configure `tmsh` to include command aliases in the list of commands in the Commands section on the command line when you use the command completion and context-sensitive help features.

To set the tmsh preference show-aliases

1. Log on to `tmsh`.
2. Type the following command:
   ```
   cli
   ```
3. Type the following command sequence:
   ```
   set preference show-aliases enabled
   ```

   When you type a question mark (?) on the command line or use the command completion feature, `tmsh` now displays command aliases in the Commands section on the command line.
Chapter 2

Using the wildcard search feature

`tmsh` supports regular expression (RE) and `glob`-based wildcard search methods. For more information about these programs, access the man page for each program using the following `tmsh` commands:

- `help regex`
- `help glob`

Using the statistics feature

You can use `tmsh` to display statistics, including historical performance statistics. You can select the format in which these statistics display, as well as reset the statistics for some of the `tmsh` components. To determine if statistics are available for a specific component, see the specific component in one of the following chapters.

Configuring preferences for and viewing statistics from `tmsh`

You can view statistics for many of the `tmsh` components using the `show` command. You can specify the units in which you want `tmsh` to display statistics. You do this using the following command syntax:

```
set / cli preference stat-units [default | kil | meg | gig | raw]
```

For example, to set `tmsh` to display statistics in parts per million, use the following command sequence:

```
set / cli preference stat-units meg
```

While you are working in `tmsh`, you can override the `stat-units` setting to display statistics for a specific component in a different unit. For example, to display the statistics for the `ltm pools` in gigabits, use the following command sequence:

```
show / ltm pool gig
```

Table 2.4 describes the units in which `tmsh` can display statistics.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>default</td>
<td>Displays data in the simplest units. For example, if the data is 1,200,001, <code>tmsh</code> displays 1.20M; however, if the data is 1,200, <code>tmsh</code> displays 1.2K. This is the default value for system statistics.</td>
</tr>
<tr>
<td>gig</td>
<td>Displays data in parts per billion.</td>
</tr>
<tr>
<td>kil</td>
<td>Displays data in parts per thousand.</td>
</tr>
</tbody>
</table>

*Table 2.4 Unit options for statistics described*
For some `tmsh` components, you can choose the level of statistics that you want to view. Table 2.5, on page 2-20, contains a description of the options you can use to display statistics, depending upon the information that you want to view. Note that all levels are not available for all components. To determine which of these options is available for a specific component, refer to the man page for the component, use the command completion feature, or see Chapter 3, *Global Commands*.

To display the statistics for a specific component at a specific level, use the following command syntax:

```
show / [module...module] [component] [detail | global | historical]
```

For example, use the following command sequence when you want to view detailed pool statistics for Local Traffic Manager pools:

```
show / ltm pool detail
```

`tmsh` also provides a historical view of system performance. You can use the `historical` option, shown in Table 2.5, on page 2-20, to display historical performance data. This option displays data that is equivalent to the performance graphs in the Configuration utility. For more information, see *Collecting performance data* in the *TMOS® Management Guide for BIG-IP® Systems*.

For example, to display statistics about current connections, and for connections that have occurred within the last 3 hours, 24 hours, 7 days, and 30 days, use the following command sequence:

```
show / sys performance connections historical
```
The components for which you can view historical data are in the system performance module. They include connections, gtm, ramcache, system, and throughput.

<table>
<thead>
<tr>
<th>Show Command Option Used</th>
<th>Statistics that display</th>
<th>Syntax of show command</th>
</tr>
</thead>
<tbody>
<tr>
<td>detail</td>
<td>Statistics for all of the components of the specified type, and the components with which these components are associated.</td>
<td><code>show / [module...module] [component] detail</code></td>
</tr>
<tr>
<td></td>
<td>Statistics for the specified component, and the components with which the specified component is associated.</td>
<td><code>show / [module...module] [component] [component_name] detail</code></td>
</tr>
<tr>
<td>global</td>
<td>Roll-up statistics for the component, and all related components.</td>
<td><code>show / [module...module] [component] global</code></td>
</tr>
<tr>
<td></td>
<td>Roll-up statistics for the specified component, and all related components.</td>
<td><code>show / [module...module] [component] [component_name] global</code></td>
</tr>
<tr>
<td>historical</td>
<td>Historical system performance statistics.</td>
<td><code>show / system performance [component] historical</code></td>
</tr>
</tbody>
</table>

*Table 2.5  Levels in which you can display statistics in `tmsh`

◆ Tip

You can also view statistics from the BIG-IP system prompt, using the following command syntax: `tmsh show / [module...module] [component] [detail \ global \ historical] [default \ kil \ meg \ gig \ raw]`
Resetting statistics

When you are evaluating the performance of your system, you might want to reset the statistics for a component. You can do that in one of two ways:

- You can reset the statistics for a type of component using this syntax:
  \texttt{reset-stats / [module...module] [component]}

- You can reset the statistics for a specific component using this syntax:
  \texttt{reset-stats / [module...module] [component] [component_name]}

\textbf{Note}

After you reset statistics, when you run the \texttt{show} command, you might see a value of \texttt{nan}. This stands for \texttt{not a number}, which indicates that no data is currently available. Wait a few moments and run the \texttt{show} command again, and in most cases the \texttt{nan} value will be replaced by an integer value.

Using grep functionality in tmsh to filter output

\texttt{grep} is a command line search utility. For more information about \texttt{grep}, see the man page using the \texttt{tmsh} command \texttt{help grep}.

To use the output of a \texttt{tmsh} command as input to the \texttt{grep} utility, use this syntax:

\texttt{[command] | grep [grep options]}

\texttt{tmsh} supports the \texttt{grep} utility options shown in Table 2.6.

\begin{table}[h]
\centering
\begin{tabular}{|c|l|}
\hline
\textbf{Supported option} & \textbf{Usage} \\
\hline
\texttt{-A}, \texttt{-B}, \texttt{-C}, \texttt{-m} & These options require a numeric argument between 0 and 4294967295. \\
\texttt{-c}, \texttt{-E}, \texttt{-G}, \texttt{-i}, \texttt{-n}, \texttt{-o}, \texttt{-P}, \texttt{-v}, \texttt{-w}, \texttt{-x} & These options do not accept arguments. Instead, the \texttt{grep} utility treats arguments for these options as either another option or a search pattern. \\
\texttt{-e} & This option requires one argument, a search pattern. \\
\texttt{[-unsupported option]} & Unsupported options preceded by a hyphen result in syntax errors. \\
\texttt{[argument]} & \texttt{tmsh} treats any argument that is not preceded by a supported option, and does not begin with a hyphen, as a search pattern preceded by \texttt{-e}. \\
& \texttt{For example, if you enter show pool | grep 10.2.3.4} within the \texttt{ltm} module, \texttt{tmsh} runs \texttt{show pool | grep -e 10.2.3.4}. \\
\hline
\end{tabular}
\caption{\texttt{grep} utility options supported in \texttt{tmsh}}
\end{table}
Creating batch mode transactions

You can issue a set of commands in a batch, and `tmsh` processes the commands as a single transaction. You enter batch mode by using the `transaction` component within the `cli module`.

When you run a set of commands in batch mode, `tmsh` does one of two things:

- Successfully runs all of the commands in the transaction.
- Does not commit any of the commands in the transaction, if the syntax of any of the commands does not pass the syntax check. In other words, `tmsh` does not partially commit a transaction.

**To create a batch mode transaction**

1. Log on to `tmsh`.
2. Type the following command sequence:
   ```
   create /cli transaction
   ```
   The `tmsh` batch mode prompt displays: `[batch mode] (tmos)#.`
3. Enter a command using the full path to the command.
   `tmsh` parses the command, and if the command passes syntax checks, `tmsh` indicates that the command has been added to the transaction.

**To view the commands in the transaction**

At the `tmsh` batch mode prompt, type:
```
list transaction
```
`tmsh` displays the commands in the transaction by numeric ID.

**To delete a command from the transaction**

At the `tmsh` batch mode prompt, type:
```
modify transaction delete [numeric ID]
```
`tmsh` deletes the command that you specify with a numeric ID. Note that the system might renumber the commands in the transaction.

**To replace a command in the transaction**

At the `tmsh` batch mode prompt, type:
```
modify transaction replace [numeric ID] [command sequence]
```
`tmsh` checks the syntax of the new command that you specify with a numeric ID, replaces the existing command identified by the numeric ID with the new command, and indicates that the transaction was updated successfully.
To insert a command in the transaction

At the tmsh batch mode prompt, type:

```
modify transaction insert [numeric ID] [command sequence]
```

*tmsh* checks the syntax of the new command that you specify to insert before a command identified by a numeric ID, renumbers the existing commands identified, and indicates that the transaction was updated successfully.

To submit the transaction

At the tmsh batch mode prompt, type:

```
submit transaction
```

*tmsh* runs the transaction. Note that if the transaction fails, *tmsh* remains in batch mode, and you can update the transaction, and then resubmit it.

To cancel the transaction

At the tmsh batch mode prompt, type:

```
delete transaction
```

*tmsh* deletes all the commands in the transaction and returns you to the tmsh prompt.

Controlling tmsh

*tmsh* includes a set of commands that you can use to change the behavior of *tmsh*, and to configure the BIG-IP system. For more information about the *tmsh* commands, see Chapter 3, *Global Commands*, or use the help command within *tmsh*.

Changing the behavior of tmsh

The options that you can use to change the behavior of *tmsh* are described in Table 2.7.

<table>
<thead>
<tr>
<th>Options</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>-a</td>
<td><em>tmsh</em> does not write commands to the command <em>glob</em> file. For more information about the command <em>glob</em> file, see <em>Using the command glob feature</em>, on page 2-10. Note that if auditing is enabled, <em>tmsh</em> continues to write commands to the audit log. For more information, see <em>Using the command audit feature</em>, on page 2-14. This option is useful when writing scripts, because it stops the scripts from filling up the command <em>glob</em> file. This option applies to the non-interactive mode only.</td>
</tr>
<tr>
<td>-c</td>
<td>Disables video highlighting in <em>tmsh</em>.</td>
</tr>
<tr>
<td>-d [ip address</td>
<td>hostname]</td>
</tr>
<tr>
<td>-h</td>
<td>Displays options you can use when accessing <em>tmsh</em> from the system shell.</td>
</tr>
</tbody>
</table>

*Table 2.7 Commands that alter the behavior of tmsh*
You can use special characters when running `tmsh` commands. Table 2.8 lists these special characters, describes how to use them, and provides examples of their usage.

<table>
<thead>
<tr>
<th>Character</th>
<th>Usage</th>
<th>Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>&quot;</strong></td>
<td>Use quotation marks around strings that contain a space or an apostrophe (single quotation mark).</td>
<td><code>create partition A description &quot;Admin’s partition&quot;</code></td>
</tr>
<tr>
<td><strong>’</strong></td>
<td>Use apostrophes around arguments or a space.</td>
<td><code>create partition A description ‘Admin’s partition’</code></td>
</tr>
<tr>
<td>\</td>
<td>Use a backslash to escape the following: quotation marks (&quot; &quot;), another backslash (), an asterisk (*), a question mark (?), brackets ([ ]), or a space. Use two backslashes when a backslash is not in quotation marks.</td>
<td><code>create gtm wideip &quot;\siterequest.com&quot;</code> <code>create gtm wideip \&quot;siterequest.com\&quot;</code> <code>create gtm wideip \siterequest.com</code> <code>create gtm wideip \siterequest\?.com</code></td>
</tr>
<tr>
<td>*</td>
<td>When escaping glob and regex special characters, use an asterisk (not between brackets) in a search string to match any string including an empty string. Use a backslash to escape an asterisk.</td>
<td><code>create gtm wideip \&quot;siterequest.com\&quot;</code></td>
</tr>
<tr>
<td>?</td>
<td>When escaping glob and regex special characters, use a question mark (not between brackets) in a search string to match a single character. Use a backslash to escape a question mark.</td>
<td><code>create gtm wideip \&quot;site\?.com\&quot;</code></td>
</tr>
</tbody>
</table>

**Table 2.8 Special character usage in tmsh**
When escaping **glob** and regex special characters, use brackets to enclose any characters that you want to include in a search string to match a single character. Use a backslash to escape square brackets.

<table>
<thead>
<tr>
<th>Character</th>
<th>Usage</th>
<th>Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>[]</td>
<td>When escaping <strong>glob</strong> and regex special characters, use brackets to</td>
<td><em>create gtm datacenter \ [site]</em></td>
</tr>
<tr>
<td></td>
<td>enclose any characters that you want to include in a search string to</td>
<td></td>
</tr>
<tr>
<td></td>
<td>match a single character. Use a backslash to escape square brackets.</td>
<td></td>
</tr>
<tr>
<td>space</td>
<td>You must escape the space character or put quotation marks around it.</td>
<td><em>create gtm pool my\ \ http\ \ pool</em></td>
</tr>
<tr>
<td></td>
<td></td>
<td><em>create gtm pool &quot;my http pool&quot;</em></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Use the vertical bar to filter output from the commands <strong>show</strong> or</td>
</tr>
<tr>
<td></td>
<td><strong>list</strong></td>
<td>*list ltm pool</td>
</tr>
</tbody>
</table>

*Table 2.8 Special character usage in tmsh (Continued)*
Introduction to command syntax

The remainder of this guide contains the command syntax for `tmsh` global commands and for configuring the `tmsh` components. You can also find information about `tmsh` command syntax in the man pages. You can display a `tmsh` man page from the `tmsh` prompt, by entering `help` followed by the full path to the component name. For example, to display the man page for the Global Traffic Manager `pool` component from the `root` module, use the following command sequence:

```
help / ltm pool
```
Global Commands

• Introducing global commands

• Alphabetical list of global commands
Introducing global commands

You can use the `tmsh` global commands within any `tmsh` module. For more information about the `tmsh` hierarchical structure, see Chapter 2, *Understanding and Using the Traffic Management Shell*.

Alphabetical list of global commands

The remainder of this chapter lists the `tmsh` global commands.
cd

Change the current working folder.

Module

All tmsh modules.

Syntax

Use the command cd to change the current working folder.

```
cd [folder name]
cd /[folder name]
```

Description

Folders are used to organize configuration. When a configuration object is created, it is associated with the current working folder. The cd command changes the current working folder to enable the user to navigate around the folder system (see sys folder).

The pwd command displays the current working directory. You can list the current working folder in the tmsh command prompt while in tmsh interactive mode (see cli preference).

Folder names are separated by a forward slash (/).

There are two built in folders:
- / is the root folder
- /Common is the default folder for creating new configuration objects

Additionally, the following directory entries:
- . is the current folder
- .. is the parent folder

Examples

Changes the current working folder to /Common:

```
cd /Common
```

Changes the current working folder to resources. In this example the resources folder is relative to the current working folder. As an example, if the current working folder was /Common, the new working folder will be /Common/resources:

```
cd resources
```
Changes the current working folder to `/resources/profiles/udp`. When specifying multiple folders, you can use tab completion to assist with filling the command line with folder names:

```
cd resources/profiles/udp
```

Makes the current working folder the root folder:

```
cd /
```

Changes the working directory by first going to the parent, and then switch to the sub-folder Alpha:

```
cd ../Alpha
```

See also

`help`, `pwd`, `sys folder`, `tmsh`
Chapter 3

**cp**

Creates a copy of a TMOS® configuration component.

**Module**

All `tmsh` modules.

**Syntax**

Use the `cp` command within a `tmsh` module to create a copy of a component that resides in that module. To create a copy component that resides in another module, use the full path to the component.

```
cp [component] [source] [destination]
cp / [module...module] [component] [source] [destination]
```

**Description**

You must provide a unique name for each component destination of the copy operation.

**Examples**

From within the `sys application` module, creates a new Application Template named `newtemplate` with the same properties as `mytemplate`:

```
cp template mytemplate newtemplate
```

From within the `sys application` module, copies the `my_script1` script to `my_script2` within the `cli` module:

```
cp / cli script my_script1 my_script2
```

**Options**

Specifies the type of the component that you want to copy:

- **module**
  Specifies the module within which resides the component that you want to copy.

- **source**
  Specifies the component to be copied.

- **destination**
  Specifies a unique name for the component that will be created as part of the copy.
See also

tmsh
create

Creates a TMOS® configuration component.

Module

All tmsh modules.

Syntax

Use the `create` command within a tmsh module to create a component that resides in that module. To create a component that resides in another module, use the full path to the component.

```
create [component] [name] [property [value]...]
create / [module...module] [component] [name] [property [value]...]
```

Description

You must provide a unique name for each component that you create.

Examples

From within the gtm module, creates a Global Traffic Manager™ pool named `pool1`:
```
create pool pool1
```

From within the ltm module, creates a Local Traffic Manager™ pool named `my_pool`:
```
create / ltm pool my_pool
```

Options

You can use the following options with the `create` command:

- **component**
  Specifies the type of component that you want to create.

- **module**
  Specifies the module within which resides the component that you want to create.

- **name**
  Specifies a unique name for the component.

- **property [value]**
  Specifies properties and their values for the component.
See also
tmsh
delete

Deletes a tmsh component.

Module

All tmsh modules.

Syntax

Use the delete command within a tmsh module to delete a component that resides in that module. To delete a component that resides in another module, use the full path to the component.

```
delete [component] [name]
dele te / [module...module] [component] [name]
```

Description

You must provide the name of the component that you want to delete.

Examples

From within the gtm module, deletes the Global Traffic Manager pool named pool1:

```
delete pool pool1
```

From within the gtm module, deletes the Local Traffic Manager pool named my_pool:

```
delete / ltm pool my_pool
```

Options

You can use the following options with the delete command:

- **component**
  Specifies the type of component that you want to delete.

- **module**
  Specifies the module within which resides the component that you want to delete.

- **name**
  Specifies a unique name for the component.
See also

tmsh
edit

Opens the specified components in an editor.

Module

All tmsh modules.

Syntax

Use the edit command to create components or modify the configuration of components using a text editor. To edit a component that resides in another module, use the full path to the component.

```
edit [component] [name...name | all]
editt [module...module] [component] [name...name | all]
```

Description

You can use the edit command to create or modify components in the auth, cli, gtm, ltm, net, sys, and wom modules, and in iRules®. You can edit the configuration of multiple objects at one time.

If you are assigned the role of Administrator, when you use the edit command, the system starts the vi editor. If you are assigned any other role, the system starts the pico/nano editor.

The system saves, in a temporary directory, the text file that you are editing, and names the file data. When you save the file and close the editor, the system checks for errors, and then prompts you with an opportunity to continue editing and resolve any errors.

When you edit an existing component that can have associations, such as a Global Traffic Manager wide IP that can have pool member associations, but the component does not currently have associations, to create the new associations, you must use the full command syntax in the text file. For the full command syntax, see the content under the Syntax headings in this chapter.

When you edit a component that has associations with components that are children of the component you are editing, the text file contains a line for the configuration of the child components that begins with the modify command, for example:

```
pools modify ( [existing pool members configurations] )
```

In this case, if you want to add or delete pool members, you must add additional lines to the text file, for example:

```
pools delete ( [pool members to delete] )
```
If you want the text file that opens to contain all of the editable properties of the component that you want to edit, you must use the all-properties option at the end of the edit command sequence; otherwise, only the non-default properties display in the text file.

Examples

From the root module, opens an editor that displays a template that you can modify to change the configuration of all Global Traffic Manager pools with names that begin with the letter a:

```
edit / gtm pool a*
```

From the gtm module, opens an editor that displays a template that you can modify to create the Data Center named new_dc:

```
edit datacenter new_dc
```

From the gtm module, opens an editor that displays a template that you can modify to change all existing datacenters with names that begin with the letter a:

```
edit datacenter a*
```

From the gtm module, opens an editor that displays a template that you can modify to create a new datacenter and edit an existing datacenter. Note that when the file opens, a template displays that you can use to create a new datacenter followed by the configuration of the existing datacenter:

```
edit datacenter new_datacenter existing_datacenter
```

From the gtm module, opens an editor that contains a template that you can modify to create an iRule named rule_1:

```
edit rule rule_1
```

◆ Note

When you are creating or editing an iRule, you must enclose the iRule syntax in brackets, for example: [...iRule...]. Note that the template includes the brackets.

Options

You can use the following options with the edit command:

♦ all
  Specifies that you want to modify all of the existing components of the specified type.

♦ component
  Specifies the type of component that you want to create or modify.

♦ module
  Specifies the module within which the component resides.
name
Specifies a unique name for each component that you want to create or modify.

See also
tmsh
**exit**

Exits a **tmsh** module or component.

**Module**

All **tmsh** modules.

**Syntax**

Use the `exit` command within a **tmsh** module or component to leave that module or component and return to the higher level of the shell structure.

```
exit
```

**Note**

To exit **tmsh** and return to the BIG-IP system prompt, use the `quit` command. For more information, see `quit`, on page 3-28.

**Description**

For more information about the structure of **tmsh**, see *Working within the tmsh hierarchy*, on page 2-3.

**See also**

**tmsh**
generate

Generate signed scripts using different algorithms for components (for example, iRules®).

Module

All tmsh modules.

Description

Use the `generate` command to generate signed scripts for components. Currently two algorithms are supported: checksum and signature.

`generate checksum <script_name>`

`generate signature <script_name> signing-key <key_name>`

See also

ltm rule, sys application template
help

Displays context-sensitive help text.

Module

All tmsh modules.

Syntax

Use the help command within a tmsh module to display information about the components that reside within that module, or at the component level to display help about the component. To display help for a component that resides in another module, use the full path to the component.

Type the question mark (?) character anywhere in tmsh to display a list of modules, components, and commands that are available within the module where you are currently working.

? help
help [module...module]
help [component]
help / [module...module] [component]

Description

You can display tmsh man pages using the help command.

Examples

From within the gtm module, displays a list of modules, components, and commands that are available:

?      

From within the gtm module, displays help about Global Traffic Manager pools:

help pool

From within the gtm module, displays help about Local Traffic Manager pools:

help / ltm pool
Options

You can use the following options with the `help` command:

- **component**
  Specifies the type of component for which you want to display help.

- **module**
  Specifies the module within which resides the component for which you want to display help.

See also

`tmsh`
install

Installs and updates components.

Module

All tmsh modules.

Description

Use the install command to install or update the following components. For the description and syntax see the help page for each component.

- sys license
- sys software hotfix
- sys software image

See also

- sys license
- sys software hotfix
- sys software image
- tmsh
list

Displays components that you have permission to view.

Module

All `tmsh` modules.

Syntax

Use the `list` command within a `tmsh` module to display the properties of the components in that module. To display the properties of the components from within another module, use the full path to the component.

```plaintext
list
list [component]
list [component] [name]
list [component] [name] [property]
list / [module] [component] [name] [property]
```

options:

- all-properties
- current-module
- non-default-properties
- one-line
- partition
- recursive

Description

When the default Read partition is `All`, use the `list` command to display all of the components that you have permission to view within a `tmsh` module. When you specify a Read partition, the `list` command displays:

- Only the components that you have permission to view in the current partition
- All of the components that are not in a partition
- All of the components in partition `Common`

Examples

From within the `gtm` module, displays the properties of all of the components in the `ltm` module, including the components in the modules that are subordinate to the `ltm` module:

```plaintext
list / ltm
```
From within the `gtm` module, displays the properties of all of the components in the `ltm` module, not including the components in the modules that are subordinate to the `ltm` module:

```
list / ltm current-module
```

From within the `gtm` module, displays the properties of all of the Global Traffic Manager pools:

```
list pool
```

From within the `gtm` module, displays the properties all of the Global Traffic Manager pools:

```
list pool all-properties
```

From within the `gtm` module, displays the monitor associated with each Global Traffic Manager pool:

```
list pool monitor
```

From within the `gtm` module, displays the properties of all Local Traffic Manager pools:

```
list / ltm pool
```

## Options

You can use these options with the `list` command:

- **all-properties**
  Displays the values of all of the properties of the specified component.

- **component**
  Specifies the component that you want to display.

- **current-module**
  Displays only the components that reside in the specified module, not the components that reside in the sub-modules of that module.

  For example, from within the `ltm` module, to display only the components in the `gtm` module, and not the components in the `gtm monitor` and `gtm settings` sub-modules, use the following command sequence: `list / gtm current-module`

- **module**
  Specifies the module within which the component that you want to display resides.

  *Note: When you use the `list` command at the module level, by default, the system does not display all of the components that reside in the specified module. To display the properties of some components you must explicitly specify the component. For example, from the `ltm` module, to display the virtual addresses for Local Traffic Manager, use the following command sequence: `list virtual-address`.*

  For more information about displaying the properties of a component, see the man page for the component.
- **name**
  Specifies the unique name of the component.

- **non-default-properties**
  Displays the values of all of the properties for which a user changed the value from the default value for the specified component.

- **one-line**
  Displays the configuration for each object on one line. Configurations that consist of scripts will not be formatted onto a single line. This includes `ltm` and `gtm` iRules and `tmsh` scripts.

- **partition**
  Displays the administrative partition within which the specified component resides.

- **property**
  Specifies the property of the component that you want to display.

- **recursive**
  Displays the components not only from the current folder but also from all sub-folders recursively.

### See also

`tmsh`
load

Replaces the running configuration of the BIG-IP system with the configuration in the specified files.

See also

save, tmsh ltm dns dns-express db, sys config, sys geoip, sys ucs
modify

Modifies a tmsh component.

Module

All tmsh modules.

Syntax

Use the modify command within a tmsh module to change a component that resides in that module. To modify a component in another module, use the full path to the component.

```
modify [component] [name] [property [value] ]...
modify / [module...module] [component] [name] [property [value] ]...
```

Description

You must provide the name of the component that you want to modify.

You can apply one or more property settings to multiple components using a single command sequence. For example, to associate the Local Traffic Manager pool named pool-1 with the virtual servers named virtual-1 and virtual-2, use the following command sequence:

```
modify ltm virtual virtual-1 virtual-2 pool pool-1
```

Examples

From within the gtm module, disables the Global Traffic Manager pool named pool1:

```
modify pool pool1 disabled
```

From within the gtm module, disables the Local Traffic Manager pool named my_pool:

```
modify / ltm pool my_pool disabled
```

Options

You can use these options with the modify command:

- **component**
  - Specifies the type of component that you want to modify.

- **module**
  - Specifies the module within which resides the component that you want to modify.
◆ **name**
   Specifies the unique name of the component that you want to modify.
◆ **property [value]**
   Specifies the properties of the component that you want to modify, and their new values.

**See also**

tmsh
mv

Renames or moves a TMOS® configuration object.

Module

All `tmsh` modules.

Syntax

Use the `mv` command within a `tmsh` module to move or rename the component that resides in that module. To move a component that resides in another module, use the full path to the component.

```
mv [component] [source] [destination]
mv / [module...module] [component] [source] [destination]
```

Description

You must provide a unique name for the source and destination of the move operation.

Currently, only the system's self device can be renamed, and it cannot be moved out of `/Common`.

Examples

Renames the device named `bigip` to `seattle32`:

```
mv cm device bigip seattle32
```

Options

You can use these options with the `modify` command:

- **component**
  
  Specifies the type of component that you want to move.

- **destination**
  
  Specifies a unique name for the component to be renamed to.

- **module**
  
  Specifies the module within which the component that you want to move resides.

- **source**
  
  Specifies the component to be moved.
See also

tmsh
publish

Finalizes changes in `wam` policy by creating a read-only copy of it.
Use the command `publish` to make `wam` policies available for usage in `wam` applications. For the description and syntax see the help page for `wam` policy.

See also

`wam policy`, `tmsh`
pwd

Displays the current working folder.

Module

All `tmsh` modules.

Syntax

Use the `pwd` command to display the current working folder.

```
pwd
```

Description

You can display the current working folder.

Examples

```
pwd
```

See also

`cd`, `help`, `sys folder`, `tmsh`
quit

Exits tmsh.

Module

All tmsh modules.

Syntax

Use the following command at the tmsh prompt to close tmsh and return to the BIG-IP system prompt.

quit

◆ Note

To exit a tmsh module or component, you use the exit command. For more information, see exit, on page 3-13.

See also

tmsh
reboot

Reboots the system or boots the system into a different volume.

Module

All tmsh modules.

Syntax

Use the `reboot` command within any tmsh module to reboot a BIG-IP system using the following syntax.

```
reboot
  options:
    slot [ [slot_id] | all ]
    volume [name]
```

Description

You can use the `reboot` command to reboot the system or cluster. If you do not specify an option, the local system reboots.

You can use the `volume` option to reboot a system into a specific volume. For a cluster, you can use the `volume` option to reboot all slots into the specified volume.

Additionally, for a cluster, you can use the `slot` option to reboot either a specific slot or all slots. Note that the `slot` option does not modify the active volume.

Examples

Immediately reboots the running image:

```
reboot
```

If the volume HD1.2 has a complete image on it, the system (or cluster) reboots into that image immediately. However, if a software installation is in progress on the volume the system reboots as soon as the installation is complete:

```
reboot volume HD1.2
```
Options

You can use these options with the `reboot` command:

- **slot**
  Reboots either a specific slot or all slots in a cluster, without changing the active volume of the slot(s). This option is only available in a clustered environment.

- **volume**
  Specifies the volume that you want to boot. The volume you specify becomes the default boot volume. You cannot specify the active volume. In a clustered environment all slots reboot into the same volume.

◆ **Note**

The `slot` and `volume` options are mutually exclusive.

See also

install, sys software hotfix, sys software image, sys software status, sys software volume, tmsh
reset-stats

Resets the statistics for the specified components.

Module

All tmsh modules.

Syntax

Use the reset-stats command within a tmsh module to reset the statistics for the specified component to zero. To reset the statistics for the specified component in another module, use the full path to the component.

reset-stats [component]
reset-stats [component] [name]
reset-stats / [module...module] [component]
reset-stats / [module...module] [component] [name]

Description

You can reset statistics for a group of components, or you can reset statistics for a specific component.

After you reset statistics, when you run the show command, you might see a value of nan. This stands for not a number, which indicates that no data is currently available. Wait a few moments and run the show command again, and in most cases the nan value will be replaced by an integer value.

It is important to note the following when you reset statistics:

- For a data center, the system also resets the statistics for the servers in that data center.
- For a Global Traffic Manager server, the system also resets the statistics for the virtual servers on that server.
- For a Global Traffic Manager pool, the system also resets the statistics for the pool members.
- For a Local Traffic Manager pool, the system also resets the statistics for the pool members.
- For a VLAN, you must reset the statistics for the trunks and interfaces associated with the VLAN.
- You cannot reset statistics for system-supplied profiles.
Examples

From within the **gtm** module, resets the statistics for all of the Global Traffic Manager pools:

```
reset-stats pool
```

From within the **ltm** module, resets the statistics for the Local Traffic Manager pool named **pool1**:

```
reset-stats pool pool1
```

From within the **gtm** module, resets the statistics for the Local Traffic Manager pool named **my_pool**:

```
reset-stats / ltm pool my_pool
```

From within the **sys performance** module, resets all performance statistics for the system:

```
reset-stats all-stats
```

Options

You can use these options with the **reset-stats** command:

- **component**
  Specifies the type of component for which you want to reset statistics.

- **module**
  Specifies the module within which resides the component for which you want to reset statistics.

- **name**
  Specifies the unique name of the component for which you want to reset statistics.

See also

**tmsh**
restart

Restarts a service on the BIG-IP system.

Module

All tmsh modules.

Syntax

Use the restart command within tmsh to restart a specified service.

```
restart
  options:
    /sys service [service name]
```

Description

You can use the restart command to restart the specified service.

Examples

Restarts the mcpd daemon:

```
restart /sys service mcpd
```

Restarts the snmpd daemon:

```
restart /sys service snmpd
```

Options

◆ Tip

*Use the command completion feature to see a list of available services.*

See also

start, stop, sys service, tmsh
run

Runs the specified program.

Module

All tmsh modules.

Syntax

Use the run command within tmsh to run a specified utility.

run

  options:
  /cli script [arguments]
  /gtm big3d_install [arguments]
  /gtm bigip_add [arguments]
  /gtm gtm_add [arguments]
  /sys config-sync
  /sys config-sync pull
  /util bash [arguments]
  /util dig [arguments]
  /util get-dossier [arguments]
  /util netstat [arguments]
  /util ping [arguments]
  /util ping6 [arguments]
  /util qkview [arguments]
  /util racoonctl [arguments]
  /util tcpdump [arguments]
  /util tracepath [arguments]
  /util tracepath6 [arguments]
  /util traceroute [arguments]
  /util traceroute6 [arguments]
  /wom diagnose-conn
  /wom verify-config

Description

You can use the run command to run the specified program or utility.

You can read about the arguments that are available for the utilities in the gtm module using the following command sequence:

  help /gtm [big3d_install | bigip_add | gtm_add]
You can read about the arguments that are available for the utilities in the `util` module using the following command sequence:

```
help /util [utility name]
```

**Note**

Some `tmsh` features, such as command completion, context-sensitive help, paging, and grep, are not available for utilities.

When you are building a batch mode transaction in `tmsh`, if you type the `run` command, the system runs the specified program immediately. It does not add the `run` command to the transaction that you are building.

### Examples

Displays the help page for the `ping` utility:

```
help /util ping
```

### Options

You can use the following options with the `run` command:

- **big3d_install**
  Installs the `big3d` daemon.

- **bigip_add**
  Specifies the BIG-IP systems that you want to add to the Global Traffic Manager configuration.

- **bash**
  Accesses the system shell.

- **config-sync**
  Synchronizes the configuration of the peer unit to the configuration of the local unit in a redundant system configuration.

- **config-sync pull**
  Synchronizes the configuration of the local unit to the configuration of the peer unit in a redundant system configuration.

- **diagnose-conn**
  Runs the specified `diagnose-conn` script, which detects the sources of network connection and performance problems in a WAN optimization configuration.

- **dig**
  Runs the specified `dig` command. The `dig` utility queries DNS name servers.

- **get-dossier**
  Runs the `get_dossier` utility for the purpose of displaying system license dossier information.
◆ **gtm_add**
   Specifies the Global Traffic Manager systems that you want to add to the Global Traffic Manager configuration.

◆ **netstat**
   Displays network connections, routing tables, interface statistics, masquerade connections, and multicast memberships.

◆ **ping**
   Runs the specified **ping** command. The **ping** utility sends ICMP echo requests to network hosts.

◆ **ping6**
   Runs the specified **ping6** command. The **ping6** utility sends ICMPv6 echo requests to network hosts.

◆ **qkview**
   Runs the specified **qkview** command. The **qkview** utility gathers diagnostic information from a BIG-IP system.

◆ **racoonctl**
   Runs the specified **racoonctl** command. The **racoonctl** utility is used to control operation of the **racoon** daemon.

◆ **tcpdump**
   Runs the specified **tcpdump** command. The **tcpdump** utility prints headers and content of network traffic.

◆ **tracepath**
   Displays the route packets take to a network host.

◆ **tracepath6**
   Displays the route packets take to an IPv6 network host.

◆ **traceroute**
   Displays the route packets take to a network host.

◆ **traceroute6**
   Displays the route packets take to an IPv6 network host.

◆ **verify-config**
   Runs the specified **verify-config** script, which detects errors in the configuration of WAN Optimization Manager™.

---

**See also**

cli script, gtm big3d_install, gtm bigip_add, gtm gtm_add, sys config-sync, tmsh, util bash, util dig, util netstat, util ping, util ping6, util qkview, util tcpdump
save

Writes the running configuration of the BIG-IP system to the specified file.

Description

You can use the `save` command to write changes that you make to the running configuration of the BIG-IP system to the specified file. You can also use this command to save an analytics report to a file on the BIG-IP system.

See also

analytics report, sys config, sys ucs, load, tmsh
send-mail

Send an email to a list of recipients containing configuration or statistical information about the BIG-IP system.

Description

You can use the send-mail command to send an analytics report from the BIG-IP system to a list of email recipients.

See also

analytics report, tmsh
show

Displays statistics for and the status of specified components.

Module

All tmsh modules.

Syntax

Use the show command within a tmsh module to display statistics for and the status of components in that module. To display statistics for and the status of components in another module, use the full path to the component.

show
show [component]
show [component] [name]
show / [module] [component] [name]

options:
  all-stats
  current-module
  (default | exa | gig | kil | meg | peta | raw | tera | yotta | zetta)
  (detail | global | historical)
  field-fmt
  running-config
  recursive

Description

You can use the show command to specify the unit value in which the system displays statistics and the type of statistics that you want the system to display.

After you reset statistics, when you run the show command, you might see a value of nan. This stands for not a number, which indicates that no data is currently available. Wait a few moments and run the show command again, and in most cases the nan value is replaced by an integer value. For more information, see reset-stats, on page 3-31.

Examples

From within the gtm module, displays statistics and status for all the components within the ltm module, but not the components in the ltm monitor, ltm persistence, and ltm profile modules:

show / ltm current-module
From within the `gtm` module, displays statistics and status for all Global Traffic Manager pools:

```
show pool
```

From within the `gtm` module, displays statistics and status for the Global Traffic Manager pool named `pool1`:

```
show pool pool1
```

From within the `gtm` module, displays statistics and status for all Local Traffic Manager pools:

```
show / ltm pool
```

From within the `gtm` module, displays global statistics and status for all Local Traffic Manager TCP profiles in the system default unit:

```
show / ltm profile tcp global
```

## Options

You can use these options with the `show` command:

- **all-stats**
  Displays all of the available system performance statistics.

- **component**
  Specifies the type of component for which you want to show statistics and status.

- **current-module**
  Displays only the components that reside in the specified module, not the components that reside in the sub-modules of that module.
  
  For example, from within the `ltm` module, to display only the components in the `gtm` module and not the components in the `gtm monitor` and `gtm settings` sub-modules, use the following command sequence: `show / gtm current-module`

- **default**
  Displays data in the simplest units. For example, if the value of the data is 1,200,001, the system displays `1.20M`; however, if the value of the data is 1,200, the system displays `1.2K`.

- **detail**
  Displays detailed data for the specified component and associated components. Note that this option is available for only a partial set of `tmsh` components.

  You can use the command completion and context-sensitive help features to determine if this option is available. For more information about these features, see `Using the command completion feature`, on page 2-7, and `help`, on page 3-15.

- **field-fmt**
  Displays data as a list of options and their values. The option names can be used to retrieve statistics and status values in a shell script, see `cli script`. 

```
- **gig**
  Displays data in parts per billion.

- **global**
  Displays global statistics for the specified component that includes statistics for all components of the specified type. Note that this option is available for only a partial set of `tmsh` components. You can use the command completion and context-sensitive help features to determine if this option is available.

- **historical**
  Displays historical statistics for the specified component. Note that this option is available for only a partial set of `tmsh` components.
  You can use the command completion and context-sensitive help features to determine if this option is available.

- **kil**
  Displays data in parts per thousand.

- **lines**
  Specifies how many lines of the log you want the system to display.

- **meg**
  Displays data in parts per million.

- **module**
  Specifies the module within which resides the component for which you want to show statistics and status.
  When you use the `show` command at the module level, by default, the system does not display all of the components that reside in the module. To display some components you must explicitly specify the component. For example, from the `ltm` module, to display the statistics for and status of the virtual addresses of Local Traffic Manager, use the following command sequence:

  ```plaintext
  show virtual-address
  ```

  For more information about displaying statistics for and the status of a component, see the man page for the component.

- **name**
  Specifies the unique name of the component for which you want to show statistics and status.

- **range**
  Specifies a date range for the logs that you want the system to display, for example:
  - **2d-4d**
    Specifies 2 - 4 days ago.
  - **3d**
    Specifies 3 days ago to now.
  - **epoch--7/25:12:00:00**
    Specifies everything older than July 25th at noon.
    Specifies between July 25th and 28th at 1:30 p.m.
◆ **raw**
  Displays raw data.

◆ **recursive**
  Displays the components not only from the current folder, but also from all sub-folders recursively.

◆ **running-config**
  Displays the running configuration of the components that you have permission to view within a **tmsh** module, if the default Read partition is **All**. If you specify a Read partition, this option displays only the running configuration of the components that you have permission to view in the current partition, all of the components that are not in partitions, and all of the components in partition Common. Note that this option is valid only for **tmsh** components that you can configure.

  The **running-config** option must be specified immediately after the `show` command, for example:

  `show running-config ltm pool`

**See also**

- cli script
- tmsh
start

Starts a service on the BIG-IP system.

Module

All tmsh modules.

Syntax

Use the `start` command within `tmsh` to start a specified service.
```
start
  options:
    /sys service [service name]
```

Description

You can use the `start` command to start the specified service.

Examples

Starts the `mcpd` daemon:
```
start /sys service mcpd
```

Starts the `snmpd` daemon:
```
start /sys service snmpd
```

Options

◆ Tip

*Use the command completion feature to see a list of available services.*

See also

`restart`, `stop`, `sys service`, `tmsh`
stop

Stops a service on the BIG-IP system.

Module

All tmsh modules.

Syntax

Use the stop command within tmsh to stop a specified service.

```
stop
  options:
    /sys service [service name]
```

Description

You can use the stop command to stop the specified service.

Examples

Stops the mcpd daemon:

```
stop /sys service mcpd
```

Stops the snmpd daemon:

```
stop /sys service snmpd
```

Options

◆ Tip

*Use the command completion feature to see a list of available services.*

See also

restart, start, sys service, tmsh
submit

Runs the transaction that you are creating.

Module

All tmsh modules.

Syntax

Use the submit command to run a transaction that you are creating.

```
submit transaction
```

Description

You can use the submit command to run a transaction, which is a series of commands that you enter in transaction mode.

For more information about creating transactions, see transaction, on page 16-31.

See also

cli transaction, tmsh
Global component

You can use the `transaction` component within all `tmsh` modules. For more information about configuring transactions, see `transaction`, on page 16-31.
analytics Module Components

- Introducing the analytics module
- Alphabetical list of components
Introducing the analytics module

You can use the tmsh components that reside within the analytics module to generate analytics reports. For more information about the tmsh hierarchical structure, see Chapter 2, Understanding and Using the Traffic Management Shell.

Alphabetical list of components

The remainder of this chapter lists the tmsh components that are available in the analytics module.
**report**

Displays an analytics report.

**Module**

analytics

**Syntax**

Show, save, or send an analytics report using the syntax shown in the following sections.

**Display**

```
show report view-by [ application | virtual | pool-member | url | client-ip | country | response-code | method | user-agent ]

options:
  drilldown {
    
      entity [ application | virtual | pool-member | url | client-ip | country | response-code | method | user-agent ]
      
      values
      
      [value ...]

  }

  field-fmt

  include-total

  include-others

  limit [number of rows]

  measures {
    [measure name ...]
  }

  order-by {
    
      measure [ measure name ]
      
      sort-type [ asc / desc ]

    }

  range [date range]
```
Save

save report view-by [ application | virtual | pool-member | url | client-ip | country | response-code | method | user-agent ]

options:
  drilldown {
    {  
      entity [ application | virtual | pool-member | url | client-ip | country | response-code | method | user-agent ]
      values 
      {  
        [value ...]
      }
    }
  }
  file [ file name ]
  format [ csv-aggregated / csv-time-series / pdf ]
  include-total
  include-others
  limit [number of rows]
  measures {
    [measure name ...]
  }
  order-by {
    {  
      measure [ measure name ]
      sort-type [ asc / desc ]
    }
  }
  range [date range]

Send

send-mail report view-by [ application | virtual | pool-member | url | client-ip | country | response-code | method | user-agent ]

options:
  drilldown {
    {  
      entity [ application | virtual | pool-member | url | client-ip | country | response-code | method | user-agent ]
      values 
      {  
        [value ...]
      }
    }
  }
  email-addresses {
Description

You can use the analytics component to generate analytics reports. You can generate an analytics report for the following entities.

- **acl-order**
  Specifies the order of the access control entries in this access control list.
  This option is required.

- **application**
  Application services.

- **virtual**
  Virtual servers.

- **pool-member**
  Pool members.

- **url**
  A URL accessed by HTTP or HTTPS.

- **client-ip**
  A single client identified by an IP address.

- **country**
  A country from which HTTP/HTTPS traffic was sent to each of the virtual servers.

- **response-code**
  An HTTP response code that was sent back to the client.

- **method**
  An HTTP method used by the client (GET, CREATE, POST, DELETE, and so on).
◆ user-agent
A browser identifier sent by the client’s browser as part of the request for URL.

Different measures are collected for each of these entities and can be a part of the report request.

Examples

Gets the average number of transactions per second of 20 virtual servers (unordered):

```
show analytics report view-by virtual measures {average-tps} limit 20
```

Gets the average number of transactions per second of the top 20 virtual servers:

```
show analytics report view-by virtual measures {average-tps} limit 20 order-by { { measure average-tps sort-type desc } } wiretap[2]
```

Gets the average number of transactions per second of the top 20 virtual servers from the last three days:

```
show analytics report view-by virtual measures {average-tps} limit 20 order-by { { measure average-tps sort-type desc } } range now-3d--now
```

Gets the average number of transactions per second of the top 10 virtual servers (ordered by average tps) on app iApp (out of several monitored) on pool members p1 and p2 (out of five monitored p1-p5) in the interval ranging from two to four days ago:

```
show analytics report view-by virtual drilldown { { entity application values { app } } { entity pool-member values { p1 p2 } } } range now-4d--now-2d measures {average-tps} limit 10 order-by { { measure average-tps sort-type DESC } }
```

Gets a distribution of requests per response code on virtual v1:

```
show analytics report view-by response-code drilldown { { entity virtual values { v1 } } } measures { transactions }
```

Gets the new sessions and average concurrent sessions of the top 5 countries, ordered by the average concurrent sessions on the application app:

```
show analytics report view-by country drilldown { { entity application values { app } } } measures { average.concurrent-sessions average-sessions } order-by { { measure average-sessions sort-type DESC } } limit 5
```

Gets the client IP address with the worst page load time:

```
show analytics report view-by client-ip drilldown { { entity virtual values { v1 } } } measures { max-page-load-time } limit 1
```

Gets the distribution of requests per application on pool members p1 and p2 ordered by the number of requests during the last week:

```
show analytics report view-by application drilldown { { entity pool-member values { p1 p2 } } } measures { transactions } order-by { { measure transactions } } range now-7d--now
```
Gets the average number of transactions per second of the top 20 virtual servers and exports to a PDF file on the BIG-IP® system:

```
save analytics report view-by virtual measures {average-tps} limit 20 order-by { { measure average-tps sort-type des } } format pdf file report.pdf
```

Gets the average number of transactions per second of the top 20 virtual servers and exports to a CSV file on the BIG-IP system:

```
save analytics report view-by virtual measures {average-tps} limit 20 order-by { { measure average-tps sort-type des } } format csv-aggregated file report.csv
```

Gets the average number of transactions per second over time of the top 10 virtual servers and exports to a CSV file on the BIG-IP system:

```
save analytics report view-by virtual measures {average-tps} limit 20 order-by { { measure average-tps sort-type desc } } format csv-time-series file report.csv
```

Gets the average number of transactions per second over time of the top 10 virtual servers and sends out an email containing the report as a PDF:

```
send-mail analytics report view-by virtual measures {average-tps} limit 20 order-by { { measure average-tps sort-type desc } } format pdf email-addresses{ some.one@someaddress.com }
```

**Options**

You can use these options with the `analytics` component:

- **device**
  Specifies a BIG-IP device on which to generate a report. (Enterprise Manager™ only)

- **device-list**
  Specifies a custom list of BIG-IP devices on which to generate a report. (Enterprise Manager only)

- **drilldown**
  Specifies specific entities that are used as a filter.

- **email-addresses**
  Specifies the list of email addresses to which the report file is sent when using the `send-mail` command.

- **file**
  Specifies the exported file path to be saved when using the `save` command. The file name should be simple (not a full path).

- **format**
  Specifies the exported file format to be saved or sent. This option must be specified when using the `save` or `send-mail` commands.

- **include-others**
  Specifies that the grand total for the measure is displayed for all entities, except for those shown in the result. This option must be used with the `drilldown` option. You can also use it with `include-others` to see the grand total.
◆ include-total
Specifies that a total summary row should be added to the analytics report. For average measures, the total value is also an average. The total value reflects only the currently displayed entities. To see the grand total, use include-others along with drilldown on the view-by entity.

◆ limit
Specifies the maximum number of rows/entities in the output result set/file. The default value is 10, not including the total row/entity. The maximum value is 1000.

◆ measures
Specifies a list of measures that can be used with the chosen entity type. The default value is transactions.
  • average-concurrent-sessions
    The average number of concurrent sessions for each entity.
  • average-new-sessions
    The average number of new sessions for each entity.
  • average-page-load-time
    The average client page load time for each entity.
  • average-request-throughput
    The average request throughput for each entity.
  • average-response-throughput
    The average response throughput for each entity.
  • average-server-latency
    The average server latency for each entity.
  • average-tps
    The average number of transactions per second for each entity.
  • client-side-sampled-transactions
    The number of transactions sampled for client side page load time.
  • max-page-load-time
    The maximum client page load time for each entity.
  • max-request-throughput
    The maximum request throughput for each entity.
  • max-response-throughput
    The maximum response throughput for each entity.
  • max-server-latency
    The maximum server latency for each entity.
  • max-tps
    The maximum number of transactions per second for each entity.
  • transactions
    The absolute number of transactions for each entity.

◆ order-by
Specifies the measures and sort type (ascending or descending) that will be used to sort the final report. The default value for measures is previously chosen measures. The default value for sort type is desc (descending).
◆ **range**
  Specifies the time/date range of the analytics information that you want to display. The given results will reflect the time range chosen here. The default value is the last hour (now--now-1h).

◆ **smtp-config-override**
  Specifies the SMTP configuration to use when sending reports by email. This overrides the default SMTP settings.

**See also**

show, save, send-mail, tmsh, ltm profile analytics
apm Module Components

- Introducing the apm module
- Alphabetical list of components
Introducing the apm module

You can use the tmsh components that reside within the apm module to configure BIG-IP® Access Policy Manager®. For more information about the tmsh hierarchical structure, see Chapter 2, Understanding and Using the Traffic Management Shell.

Alphabetical list of components

The remainder of this chapter lists the tmsh components that are available in the apm module.
acl

Manages an access control list (ACL).

Module

apm

Syntax

Configure the acl component within the apm module using the syntax shown in the following sections.

Create/Modify

create acl [name]
modify acl [name]

options:
  acl-order [integer]
description [[string] | none]
entries {
  
  options:
    action [allow | continue | discard | reject | unspec]
dst-end-port [[service] | none]
dst-start-port [[service] | none]
dst-subnet [[ip addr] | [[ip addr] [mask]]
host [[string] | none]
log [config | none | packet | summary | verbose]
paths [[string] | none]
protocol [integer]
scheme [any | http | https]
src-end-port [[service] | none]
src-start-port [[service] | none]
src-subnet [[ip addr] | [[ip addr] [mask]]

  }
}

path-match-case [false | true]
type [dynamic | static]

Display

list acl
list acl [ [ [name] | [glob] | [regex] ] ... ]
The `acl` component is used to configure a set of restrictions associated with a resource or favorite that defines access for users and groups.

### Examples

Creates the static access control list named **MyACL** that is the third ACL in the list of ACLs in the Visual Policy editor, and adds an access control entry that allows traffic using the default source IP address and the default destination IP address:

```plaintext
create acl MyACL { acl-order 3 entries src-start-port ip default inet dst-end-port ip default inet action allow }
```

Displays a list of ACLs that includes the attributes of each ACL:

```plaintext
list acl all-properties
```

Deleting the **MyACL** access control list:

```plaintext
delete acl MyACL
```
entries
Configures an entry for an access control list.

The options are:

- **action**
  Specifies the action that an access control list takes when this access control list entry is encountered. This option is required. You can specify one of the following actions:
  - **allow**
    Allows traffic.
  - **continue**
    Skips checking against the remaining access control list entries in this access control list, and continues evaluation at the next access control list.
  - **discard**
    Drops packets silently.
  - **reject**
    Drops a packet and sends TCP RST on TCP flows or proper ICMP messages on UDP flows. Silently drops a packet on other protocols.

- **dst-end-port**
  Specifies the destination IP address and network mask of the access control list entry. The default value is 0.

- **dst-start-port**
  Specifies the source port or range of ports of the access control list entry.

- **dst-subnet**
  Specifies the destination subnet.

- **host**
  Specifies the host name of the access control list entry.

- **log**
  Specifies the log level that is logged when actions of this type occur. Your options are:
  - **config**
    Logs the configuration of a matched entry.
  - **none**
    Logs nothing. This is the default value.
  - **packet**
    Logs a matched packet.
  - **summary**
    Logs the name and entry number of a matched access control list and access control list entry.
  - **verbose**
    Logs everything.
  - **paths**
    Specifies an L7 access control list of matching URL paths.
• **protocol**
  Specifies the protocol number (TCP=6, UDP=17) of the access control list entry. The default value is 0.

• **src-end-port**
  Specifies the source IP address and network mask of the access control list entry.

• **src-start-port**
  Specifies the source port or range of ports of the access control list entry.

• **src-subnet**
  Specifies the source subnet.

◆ **name**
  Specifies the name of the access control list. This setting is required.

◆ **partition**
  Displays the partition within which the object resides. The default value is Common.

◆ **path-match-case**
  Indicates whether the path is case sensitive. The default value is true.

◆ **type**
  Specifies the type of access control list. The available types are static and dynamic. The default value is static.

See also

create, delete, edit, list, modify, show, tmsh
apm aaa Module Components

- Introducing the apm aaa module
- Alphabetical list of components
Introducing the apm aaa module

You can use the tmsh components that reside within the apm aaa module to configure BIG-IP® Access Policy Manager®. For more information about the tmsh hierarchical structure, see Chapter 2, Understanding and Using the Traffic Management Shell.

Alphabetical list of components

The remainder of this chapter lists the tmsh components that are available in the apm aaa module.
active-directory

Manages an authentication access policy (AAA) Active Directory® server.

Module

apm aaa

Syntax

Configure the active-directory component within the aaa module using the syntax shown in the following sections.

Create/Modify

create active-directory [name]
modify active-directory [name]

options:
  admin-encrypted-password [[string] | none]
  admin-name [[string] | none]
  description [[string] | none]
  domain [[string] | none]
  domain-controller [[string] | none]
  domain-controller [add | delete | modify | replace-all-with] {
    [name] {
      ip [ip address]
    }
  }
  domain-controllers none
  pool [name]
  timeout [[integer] | immediate | indefinite]

edit active-directory [ [ [name] | [glob] | [regex] ] ... ]

options:
  all-properties
  non-default-properties

Display

list active-directory
list active-directory [ [ [name] | [glob] | [regex] ] ... ]

show running-config active-directory
show running-config active-directory [ [ [name] | [glob] | [regex] ] ... ]

options:
all-properties
app-service
non-default-properties
one-line
partition
show active-directory
show active-directory [name]

Delete

delete active-directory [name]

Description

You can use the active-directory component to manage an AAA Active Directory server.

The Active Directory is a network structure supported by Windows® 2000, or later, that provides support for tracking and locating any object on a network.

Examples

Creates the AAA Active Directory server named MyADserver in the company.com domain, sets the administrator logon name to administrator and the administrator password to !My123Password, and sets the Key Distribution Center to company.com:

create active-directory MyADserver { domain-controller "server01.company.com" domain "company.com" admin-name "administrator" admin-encrypted-password "!My123Password" }

Displays a list of all AAA Active Directory servers on the system:

show active-directory all

Deletes the AAA Active Directory server named MyActiveDirectoryServer from the system.

delete active-directory MyActiveDirectoryServer

Options

You can use these options with the active-directory component:

◆ admin-encrypted-password
   Specifies the password associated with admin name. This option is required only when you are using an Active Directory Query agent with this Active Directory server object.
- **admin-name**
  Specifies the user name that has administrative permissions on an AAA Active Directory server. This option is required only when you are using an Active Directory Query agent with this Active Directory server object.

- **description**
  Specifies a description for the component. The default value is **none**.

- **domain**
  Specifies the Active Directory domain name. This setting is required.

- **name**
  Specifies the name of an AAA Active Directory server. This setting is required.

- **domain-controller**
  Specifies the fully qualified domain name (FQDN) of the domain controller for the domain specified in the **domain** option. The default value is **none**.

- **domain-controllers**
  Adds, deletes, or replaces a set of domain controllers; you must specify a fully qualified domain name for each entry. You can configure the following options for each domain controller:
  - **ip** - An IP address for specified domain controller entry.
  - **pool** - Specifies the name of the pool with which the server is associated. The default is **none**.

- **partition**
  Displays the partition within which the component resides. The default value is **Common**.

- **timeout**
  Specifies a timeout interval (in seconds) after which an AAA Active Directory server closes a connection. The default value is **15**.

See also

apm, create, delete, edit, list, modify, show, tmsh
crldp

Configures a Certificate Revocation List Distribution Point (CRDLP) server object for implementing a CRDLP authentication module.

Module

apm aaa

Syntax

Configure the crldp component within the aaa module using the syntax shown in the following sections.

Create/Modify

create crldp [name]
modify crldp [name]

options:
  address [ip addr]
  allow-nullcrl [true | false]
  base-dn [[string> | none]
  cache-expire [[integer] | none]
  connection-timeout [[integer] | none]
  description [[string> | none]
  pool [name]
  port [[integer] | none]
  reverse-dn [true | false]
  use-issuer [true | false]
  use-pool [enabled | disabled]
  verify-sig [true | false]

edit crldp | [glob] | [regex] ] ... ]

options:
  all-properties
  non-default-properties

Display

list crldp
list crldp [ [ [name] | [glob] | [regex] ] ... ]
show running-config crldp
show running-config crldp [ [ [name] | [glob] | [regex] ] ... ]

options:
  all-properties
  app-service
non-default-properties

one-line

partition

show crldp
show crldp [name]

Delete

delete crldp [name]

Description

Configure a CRLDP authentication server, and then assign the server to the CRLDP auth agent in your access policy.

Examples

Creates a CRLDP server named aaa-ldap-2027:

create crldp aaa-ldap-2027 { address 172.27.32.60 allow-nullcrl false base-dn
DC=net,DC=aina,DC=test cache-expire 1000 connection-timeout 15 description none
partition Common pool aaa-ldap-2027-pool port ldap reverse-dn true use-issuer false
use-pool disabled verify-sig true }

Deletes the CRLDP server named my_crldp_server:

delete crldp server my_crldp_server

Options

You can use these options with the crldp component:

- **address**
  Specifies the IP address of the server. This option is required.

- **allow-nullcrl**
  Specifies whether to consider a null CRL from the CRLDP server a successful authentication. The default value is false.

- **base-dn**
  Specifies the LDAP base directory name for certificates that specify the CRL distribution point in directory name (dirName) format. Used when the value of the X.509v3 attribute crlDistributionPoints is of type dirName. In this case, the BIG-IP system attempts to match the value of the crlDistributionPoints attribute to the Base DN value. An example of a Base DN value is cn=lxxy,dc=f5,dc=com.

- **cache-expire**
  Specifies (in seconds) an update interval for CRL distribution points. The update interval for distribution points ensures that CRL status is checked.
at regular intervals, regardless of the CRL timeout value. This helps prevent CRL information from becoming outdated before the Access Policy Manager checks the status of a certificate.

- **connection-timeout**
  Specifies the number of seconds of inactivity the system allows before the connection times out. The default value is 15.

- **description**
  Specifies a unique description for the server. The default value is none.

- **partition**
  Displays the partition within which the component resides.

- **pool**
  Specifies the name of the pool with which the server is associated.

- **port**
  Specifies the CRLDP service port. The default value is 389.

- **reverse-dn**
  Specifies in which order the system is to attempt to match the Base DN value to the value of the X.509v3 attribute crlDistributionPoints. Possible values are enabled and disabled. When set to enabled, the system matches the base DN from left to right, or from the beginning of the DN string, to accommodate dirName strings in certificates such as C=US,ST=WA,L=SEA,OU=F5,CN=xxx. The default value is false.

- **use-issuer**
  Specifies whether the CRL distribution point is extracted from the certificate of the client certificate issuer. The default value is false.

- **use-pool**
  Enables or disables high availability between CRLDP servers. When enabled, Access Policy Manager sends CRLDP authentication requests for the associated CRLDP auth agent to the virtual server, and standard pool behavior is used to implement high availability for CRDLP.

- **verify-sig**
  Specifies whether the signature on the received CRL is verified. The default if true.

See also

apm, create, delete, edit, list, modify, show, tmsh
http

Specifies an HTTP server configuration used for authentication.

Module

apm aaa

Syntax

Configure the http component within the aaa module using the syntax shown in the following sections.

Create/Modify

create http [name]
modify http [name]

options:
- description [[string] | none]
- follow-redirect [integer]
- form-action [[string] | none]
- form-fields [[string] | none]
- form-method [get | post]
- form-params [[string] | none]
- form-password [[string] | none]
- form-username [[string] | none]
- start-uri [[string] | none]
- success-match-type [url | cookie | string]
- success-match-value [[string] | none]

edit http [ [ [name] | [glob] | [regex] ] ... ]

options:
- all-properties
- non-default-properties

Display

list http
list http [ [ [name] | [glob] | [regex] ] ... ]

show running-config http
show running-config http [ [ [name] | [glob] | [regex] ] ... ]

options:
- all-properties
- app-service
- non-default-properties
You can use the http component to create and manage AAA HTTP servers.

Examples

Creates an HTTP authentication server named MyHttpServer with a starting URI of http://mycompany.com:

```
create http MyHttpServer { start-uri "http://mycompany.com/" }
```

Displays a list of AAA HTTP servers:

```
show http
```

Deletes the Myhttpauthserver AAA HTTP server:

```
delete http Myhttpauthserver
```
◆ **form-method**  
   Specifies the form method you want to use for the form-based HTTP authentication. The value is either **GET** or **POST**. The default value is **POST**. However, if you specify **GET**, the Access Policy Manager will force the authentication using HTTP GET rather than perform authentication using form-based POST.

◆ **form-password**  
   Specifies the parameter names used by the form you are sending the POST request to.

◆ **form-username**  
   Specifies the parameter names used by the form you are sending the POST request to.

◆ **name**  
   Specifies the name of the aaa http server. This option is required.

◆ **partition**  
   Displays the partition within which the component resides. The default value is **Common**.

◆ **start-uri**  
   Specifies a URL resource, for example,  
   http://plum.tree.lab2.sp companynet.com/.  
   This resource must respond with a challenge to a non-authenticated request.

◆ **success-match-type**  
   Specifies the method your authentication server uses and determines the option definition used for this field. The field toggles according to your selection.
   - **cookie**  
     Specifies a cookie name is required.
   - **last**
   - **string**  
     Specifies a specific string is required.
   - **url**  
     Specifies a URL is required.

◆ **success-match-value**  
   Specifies the URL, cookie, or specific string used for the specific success match type you see.

---

**See also**

apm, create, delete, edit, list, modify, show, tmsh
kerberos

Configures a Kerberos server.

Module

apm aaa

Syntax

Configure the kerberos component within the aaa module using the syntax shown in the following sections.

Create/Modify

create kerberos [name]
modify kerberos [name]
  options
    auth-realm [[string] | none]
    keytab-file-obj [[string] | none]
    service-name [[string] | none]
edit kerberos | [glob] | [regex] ] ... ]
  options:
    all-properties
    non-default-properties

Display

list kerberos
list kerberos [ [ [name] | [glob] | [regex] ] ... ]
show running-config kerberos
show running-config kerberos [ [ [name] | [glob] | [regex] ] ... ]
  options:
    all-properties
    app-service
    non-default-properties
    one-line
    partition
show kerberos
show kerberos [name]

Delete

delete kerberos [name]
Description

You can use the kerberos component to create and manage AAA Kerberos servers. Use the Kerberos authentication server to configure authentication for the Access Policy Manager. A client retrieves credentials from the domain controller and passes those credentials to the Access Policy Manager. Then Access Policy Manager uses the value in the keytab-file-obj option of the Kerberos AAA server object to verify the credentials. Access Policy Manager system does not have to reside in the domain.

Examples

Deletes the server named my_kerberos:

delete kerberos my_kerberos

Options

You can use these options with the crldp component:

- **auth-realm**
  Specifies a Kerberos auth realm name (administrative name), such as user@realm.com to establish the boundaries within which an authentication server has the authority to authenticate a user, host, or service. Kerberos clients manually map DNS domain names to Kerberos realm names. This option is required.

- **keytab-file-obj**
  Specifies a keytab file that contains the keys (derived from the Kerberos password) that the server uses to authenticate the client. This option is required.

- **name**
  Specifies the name of an AAA RADIUS server. This option is required.

- **partition**
  Displays the partition within which the component resides.

- **service-name**
  Specifies the Kerberos service name defined inside KDC in the format service name/hostname@kerberosrealm. This option is required, for example, HTTP.

See also

apm, create, delete, edit, list, modify, show, tmsh
kerberos-keytab-file

Manages a Kerberos Keytab file.

Module

apm aaa

Syntax

Configure the kerberos-keytab-file component within the aaa module using the syntax shown in the following sections.

Create/Modify

create kerberos-keytab-file [name]
modify kerberos-keytab-file [name]
  options:
    source-path [string]
edit kerberos-keytab-file | [glob] | [regex] | ... |
  options:
    all-properties
    non-default-properties

Display

list kerberos-keytab-file
list kerberos-keytab-file [ [ [name] | [glob] | [regex] ] ... ]
show running-config kerberos-keytab-file
show running-config kerberos-keytab-file [ [ [name] | [glob] | [regex] ] ... ]
  options:
    all-properties
    app-service
    non-default-properties
    one-line
    partition
show kerberos-keytab-file
show kerberos-keytab-file [name]

Delete

delete kerberos-keytab-file [name]
Description

You can use the `kerberos-keytab-file` component to create and manage a Kerberos Keytab file.

Examples

Creates a Kerberos Keytab file name `my_keytab` located at `root/apmkeytab`:

```
create kerberos-keytab-file my_keytab { source-path file:/root/apmkeytab }
```

Displays a list of Kerberos Keytab files:

```
show kerberos-keytab-file
```

Deletes the Kerberos Keytab file name `my_keytab`:

```
delete kerberos-keytab-file my_keytab
```

Options

You can use these options with the `crldp` component:

- `source-path`
  Specifies the location of the Kerberos Keytab file.

- `partition`
  Displays the partition within which the component resides.

See also

`apm, create, delete, edit, list, modify, show, tmsh`
ldap

Manages a Kerberos Keytab file.

Module

apm aaa

Syntax

Configure the ldap component within the aaa module using the syntax shown in the following sections.

Create/Modify

create ldap [name]
modify ldap [name]

options:
address [[ip addr] | none]
admin-dn [[string] | none]
admin-encrypted-password [[string] | none]
description [[string] | none]
is-ldaps [false | true]
pool [name]
port [[service] | none]
serverssl-profile [none | serverssl | serverssl-insecure-compatible | wom-default-serverssl]
timeout [integer]
use-pool [enabled | disabled]

edit ldap [ [ [name] | [glob] | [regex] ] ... ]

options:
all-properties
non-default-properties

Display

list ldap
list ldap [ [ [name] | [glob] | [regex] ] ... ]
show running-config ldap
show running-configure ldap [ [ [name] | [glob] | [regex] ] ... ]

options:
all-properties
app-service
non-default-properties
one-line
Chapter 6

**Partition**

show ldap

**Delete**

delete ldap [name]

**Description**

You can use the ldap component to create and manage an AAA LDAP server.

**Examples**

Creates the AAA LDAP server named MyLDAPServer that is assigned the IP address 172.30.6.144 and the cn=administrator, cn=users, dc=company, dc=companynet, dc=com admin dn with a password of !MyPassword:

```plaintext
create ldap MyLDAPServer {
  address 172.30.6.144
  admin-dn "cn=administrator,cn=users,dc=company,dc=companynet,dc=com"
  admin-encrypted-password "!MyPassword"
}
```

Displays a list of AAA LDAP servers:

```plaintext
show ldap all
```

Deletes the AAA LDAP server named MyLDAPServer from the system:

```plaintext
delete ldap MyLDAPServer
```

**Options**

You can use these options with the ldap component:

- **address**
  
  Specifies the IP address of an AAA LDAP server. This option is required.

- **admin-dn**
  
  Specifies the Container Distinguished Name (DN) to use for authentication. This option is required.

- **admin-encrypted-password**
  
  Specifies the password for admin name. This option is required.

- **description**
  
  Specifies a unique description for the server. The default value is **none**.
◆ **is-ldaps**
   Specifies whether to use the LDAPS protocol during authentication. If true, you must also specify the option **serverssl-profile**.

◆ **name**
   Specifies the name of the AAA server. This option is required.

◆ **partition**
   Displays the partition within which the component resides.

◆ **pool**
   Specifies the name of the pool with which the server is associated. The default value is **none**.

◆ **port**
   Specifies the port number of the AAA LDAP server. The default value is **ldap**. This option is required.

◆ **serverssl-profile**
   Specifies the server side SSL profile. LDAPS is achieved by directing LDAP traffic over a virtual server that uses a server side SSL to communicate with the LDAP server.
   
   The options are:
   
   - serverssl
   - serverssl-insecure-compatible
   - wom-default-serverssl

◆ **timeout**
   Specifies a timeout interval (in seconds) for the AAA server after which the server closes a connection. The default value is **15**.

◆ **use-pool**
   Enables or disables high availability between pool members. When enabled, the Access Policy Manager sends AAA requests for the associated policy item to the virtual server, and standard pool behavior is used to implement high availability for CRDLP.

---

**See also**

apm, create, delete, edit, list, modify, show, tmsh
**oam**

Manages an AAA Oracle® Access Manager server.

**Module**

`apm aaa`

**Syntax**

Configure the `oam` component within the `aaa` module using the syntax shown in the following sections.

**Create/Modify**

```plaintext
create oam [name]
modify oam [name]
```

**options:**

- `access-server-hostname` [[string] | none]
- `access-server-name` [[string] | none]
- `access-server-port` [[integer] | none]
- `access-server-retries` [integer]
- `accessgate-encrypted-password` [[string] | none]
- `accessgates` [add | delete | modify | replace-all-with] {
  [name]
}
- `action` [config-accessgate | noop]
- `admin-id` [[string] | none]
- `admin-password` [[string] | none]
- `description` [[string] | none]
- `enable` [false | true]
- `global-access-protocol-passphrase` [[string] | none]
- `transport-security-mode` [cert | open | simple]

```plaintext
edit oam | [glob] | [regex] ] ... ]
```

**options:**

- `all-properties`
- `non-default-properties`

**Display**

```plaintext
list oam
list oam [ [ [name] | [glob] | [regex] ] ... ]
```

```plaintext
show running-config oam
```

```plaintext
show running-config oam [ [ [name] | [glob] | [regex] ] ... ]
```
options:
   all-properties
   app-service
   non-default-properties
   one-line
   partition

show oam
show oam [name]

Delete
   
   delete oam [name]

Description

You can use the **oam** component to create and manage an AAA Oracle Access Manager (OAM) server.

Examples

Creates the AAA OAM server named **oam10g** accessing the web gate **oam10gwebgate1** on the Access Server **accessSrv1** at host name **www.localcorp.biz** on port **6021**. The server retries connections zero times:

```
create oam oam10g {
   access-server-hostname www.localcorp.biz
   access-server-name accessSrv1
   access-server-port 6021
   access-server-retries 0
   accessgates {
      oam10gwebgate1 {
         encrypted-password [string]
      }
   }
   admin-id firstname.lastname
   admin-password "[string]"
   global-access-protocol-passphrase "[string]"
   transport-security-mode simple
}
```

Displays a list of all AAA Oracle Access Manager servers on the system:

```
show aaa oam all
```

Deletes the AAA Oracle Access Manager server named **MyOAMServer** from the system:

```
delete aaa oam MyOAMServer
```
Chapter 6

Options

You can use these options with the oam component:

- **access-server-hostname**
  Specifies the IP address or FQDN of the Oracle Access Manager server. This option is required.

- **access-server-name**
  Specifies the name of the Oracle Access Manager server. This option is required.

- **access-server-port**
  Specifies the port of the Oracle Access Manager server. The default value is **6021**.

- **access-server-retries**
  Specify the number of times you want the access gate to attempt to connect to the Oracle Access Manager server when the action option is set to **config-accessgate**. The default value is **0** (zero).

- **accessgates**
  Specifies the ID of the access gate or web gate on the OAM Server. The system supports the use of multiple access gates/web gates as long as they are from the same OAM server.

- **action**
  Specifies the Oracle Access Manager action type. Actions allow you to pass user profile information or to redirect the user's browser to another site. For more information on Actions, refer to the *Oracle® Access Manager Access Administration Guide*.

  The options are:
  - **config-accessgate**
    Specifies that you want the system to use the configure AccessGate tool.
  - **noop**
    Specifies "no operation performed." This is the default.

- **admin-id**
  Specifies the administrator ID required by the Oracle Access Manager server. This option is required.

- **admin-password**
  Specifies the administrator password required by the Oracle Access Manager server. The default value is **none**.

- **description**
  Specifies a unique description for the Oracle Access Manager server. The default value is **none**.

- **enable**
  Specifies whether you want to enable the server. The default value is **true**.

- **global-access-protocol-passphrase**
  Specifies a global passphrase for all Oracle components. The default value is **none**.
◆ **name**  
Specifies the name of an AAA Oracle Access Manager server. This setting is required.

◆ **transport-security-mode**  
Specifies the transport security level for the communication between Oracle components and Access Policy Manager.  
The options are:

  • **open**  
  Communication is not encrypted for protection. Use this mode when security is not an issue.

  • **simple**  
  Communication is encrypted with Oracle Access Manager's internal CA. Simple mode encrypts communications using Transport Layer Security. See RFC 2246 (TLS v1). This mode is less secure than **cert** mode. Use this mode if you have some security concerns but do not want to manage your own CA.

  • **cert**  
  Communication is encrypted with an external CA. Use **cert** mode if you want different certificates on OAM servers and webgates and you have a trusted third party CA. Oracle Access Manager components use X.509 digital certificates in PEM format only.

**See also**

apm, create, delete, edit, list, modify, show, tmsh
**ocsp**

Configures Online Certificate System Protocol (OCSP) responder objects.

**Module**

`apm aaa`

**Syntax**

Configure the `ocsp` component within the `aaa` module using the syntax shown in the following sections.

**Create/Modify**

```
create ocsp [name]
modify ocsp [name]
```

**options:**

- `allow-certs [true | false]`
- `ca-file (<file name> | none)`
- `ca-path (<file name> | none)`
- `cert-id-digest (sha1 | md5)`
- `chain [true | false]`
- `check-certs [true | false]`
- `explicit-ocsp [true | false]`
- `ignore-aia [true | false]`
- `intern [true | false]`
- `nonce [true | false]`
- `sign-digest (sha1 | md5)`
- `sign-key (<file name> | none)`
- `sign-key-passphrase (<string> | none)`
- `sign-other (<file name> | none)`
- `signer (<file name> | none)`
- `status-age <number>`
- `trust-other [true | false]`
- `url (<string> | none)`
- `va-file (<file name> | none)`
- `validity-period <number>`
- `verify [true | false]`
- `verify-cert [true | false]`
- `verify-other (<string> | none)`
- `verif-sig [true | false]`
edit ocsp | [glob] | [regex] | ... |
  options:
    all-properties
    non-default-properties

Display

list ocsp
list ocsp [ [ [name] | [glob] | [regex] ] | ... ]
show running-config ocsp
show running-config ocsp [ [ [name] | [glob] | [regex] ] | ... ]
  options:
    all-properties
    app-service
    non-default-properties
    one-line
    partition
show ocsp
show ocsp [name]

Delete

delete ocsp [name]

Description

To implement the SSL OCSP authentication module, create an OCSP responder object and assign it to the OCSP auth agent in your access policy.

Options

You can use these options with the `ocsp` component:

- **allow-certs**
  Specifies whether the addition of certificates to an OCSP request is enabled. The default value is `true`.

- **ca-file**
  Specifies the name of the certificate file object containing trusted CA certificates used to verify the signature on the OCSP response. The default value is `none`.

- **ca-path**
  Specifies the path to the trusted CA certificates used to verify the signature on the OCSP response. The default value is `none`. 
◆ **cert-id-digest**
The cert ID digest is part of the OCSP protocol. The OCSP client (in this case, the BIG-IP system) calculates the cert ID using a hash of the Issuer and serial number for the certificate that it is trying to verify.

The options are:

- **sha1**
  Newer algorithm that provides a higher security level with a 160 bit hash length. This is the default.

- **md5**
  Older algorithm with a 128 bit hash length.

◆ **chain**
  Specifies whether the system constructs a chain from certificates in the OCSP response. The default value is **true**.

◆ **check-certs**
  Specifies whether the Local Traffic Manager™ system makes additional checks to see if the signer's certificate is authorized to provide the necessary status information. Use this option only for testing purposes. The default value is **true**.

◆ **explicit-ocsp**
  Specifies whether the BIG-IP system explicitly trusts that the OCSP response signer's certificate is authorized for OCSP response signing. If the signer's certificate does not contain the OCSP signing extension, setting this option to **true** causes a response to be untrusted. The default value is **true**.

◆ **ignore-aia**
  Specifies whether to ignore the URL contained in the certificate's AIA fields, and to always use the URL specified by the responder instead. The default value is **false**.

◆ **intern**
  Specifies whether to ignore certificates contained in an OCSP response when searching for the signer's certificate. When you set this option to **true**, you must also specify the signer's certificate using either the **verify-other** or **va-file** option. The default value is **true**.

◆ **name**
  Specifies a unique name for the component. This option is required.

◆ **nonce**
  Specifies whether a nonce will be sent in an OCSP request. When set to **false**, the request is sent without a nonce. The default value is **true**.

◆ **partition**
  Displays the partition within which the OCSP responder object resides.

◆ **sign-digest**
  Specifies the algorithm (**md5** or **sha1**) used to sign a request using a signing certificate and key. The default value is **sha1**. If you use this option, you must also set the **sign-key** and **sign-key-passphrase** options.
◆ **sign-key**
   Specifies the key used to sign an OCSP request. If you use this option, you must also set the `sign-digest` and `sign-key-passphrase` options. The default value is none.

◆ **sign-key-passphrase**
   Specifies the passphrase for the signing key. If you use this option, you must also set the `sign-digest` and `sign-key` options. The default value is none.

◆ **sign-other**
   Specifies additional certificates to add to an OCSP request. The options are `default.crt` and `ca-bundle.crt`. The default value is none.

◆ **signer**
   Specifies the certificate used to sign an OCSP request. If the certificate is specified but the key is not specified, then the private key is read from the same file as the certificate. If neither the certificate nor the key is specified, then the request is not signed. If the certificate is not specified and the key is specified, then the configuration is considered to be invalid. The default value is none.

◆ **status-age**
   Species the amount of time (in seconds) to compare to the `notBefore` value of a status response. Use this option only when a status response does not include the `notAfter` field. The default value is 0 (zero).

◆ **trust-other**
   Specifies whether the BIG-IP system trusts the certificates specified using the `verify-other` option. The default value is false.

◆ **url**
   Specifies the URL used to contact the OCSP service on the responder. This option is required. The default value is none.

◆ **va-file**
   Specifies the name of the file containing explicitly-trusted responder certificates. Use this option when the responder is not covered by the certificates already loaded into the responder's CA store. The default value is none.

◆ **validity-period**
   Specifies an acceptable error range in seconds. Use this option when the OCSP responder clock and a client clock are not synchronized, which could cause a certificate status check to fail. This value must be a positive number. This option is required. The default value is 300.

◆ **verify**
   Specifies whether verification of an OCSP response signature or the nonce values is enabled. Use this option only for debugging purposes. The default value is true.

◆ **verify-cert**
   Specifies whether the BIG-IP system verifies the certificate in the OCSP response. The default value is true.
◆ verify-other
   Specifies the name of the file used to search for an OCSP response
   signing certificate when the certificate has been omitted from the
   response. The default value is none.

◆ verify-sig
   Specifies whether the BIG-IP system checks the signature on the OCSP
   response. Use this option only for testing purposes. The default value is
   true.

See also

apm, create, delete, edit, list, modify, show, tmsh
radius

Manages an AAA RADIUS server.

Module

apm aaa

Syntax

Configure the radius component within the aaa module using the syntax shown in the following sections.

Create/Modify

create radius [name]
modify radius [name]

options:
  acct-port [integer]
  address [[[ip addr] | none]
  auth-port [integer]
  description [[[string] | none]
  mode [acct | auth | both | none]
  nas-ip-address [[[ip addr] | none]
  nas-ipv6-address [[[ip addr] | none]
  pool [[[string] | none]
  retries [integer]
  secret [string]
  timeout [[[integer] | immediate | indefinite]
  use-pool [enabled | disabled]

edit radius | [glob] | [regex] ] ... ]

options:
  all-properties
  non-default-properties

Display

list radius
list radius [ [ [name] | [glob] | [regex] ] ... ]
show running-config radius
show running-config radius [ [ [name] | [glob] | [regex] ] ... ]

options:
  all-properties
  app-service
non-default-properties
one-line
partition
show radius
show radius [name]

Delete

delete radius [name]

Description

You can use the radius component to create and manage an AAA RADIUS server.

Examples

Creates the AAA RADIUS server named rad_auth that has an IP address of 172.30.6.144 and has a shared secret of test:

create rad_auth { address 172.30.6.144 secret "test" use-pool "disabled" }

Displays a list of all AAA RADIUS servers on the system:

show radius all

Deletes the AAA RADIUS server named MyRadiusServer from the system:

delete radius MyRadiusServer

Options

You can use these options with the radius component:

◆ acct-port
    Specifies the port number of the external AAA RADIUS accounting server. The default value is radius-acct.
◆ address
    Specifies the IP address of the AAA RADIUS server. This option is required.
◆ auth-port
    Specifies the port number for the service. The default value is radius. This option is required.
◆ description
    Specifies a unique description for the AAA RADIUS server. The default value is none.
◆ **mode**  
Specifies the configuration mode you want to use for RADIUS authentication. Note that you cannot modify the mode once you create the server.

The options are:

- **acct**  
  Configures the system to perform only RADIUS accounting. Use this option to pass accounting information about your users to the external RADIUS accounting server.

- **auth**  
  Configures the system to perform only RADIUS authentication. Use this option to authenticate your users through a RADIUS server.

- **both**  
  Configures the system to perform both RADIUS authentication and RADIUS accounting simultaneously.

- **none**  
  Configures the system to perform neither RADIUS authentication nor RADIUS accounting.

◆ **name**  
Specifies the name of an AAA RADIUS server. This option is required.

◆ **nas-ip-address**  
Specifies an IP address as RADIUS attribute 4 that you can configure without changing the source IP address in the IP header of the RADIUS packets. Use this option in situations where you are using a network-attached storage (NAS) cluster to be recognized as a single RADIUS client.

◆ **nas-ipv6-address**  
Specifies an IPv6 address as RADIUS attribute 4 that you can configure without changing the source IP address in the IP header of the RADIUS packets. Use this option in situations where you are using a NAS cluster to be recognized as a single RADIUS client.

◆ **partition**  
Displays the partition within which the component resides.

◆ **pool**  
Specifies the name of the pool to which this server belongs. The default value is **none**.

◆ **retries**  
Specifies the number of times the BIG-IP system tries to make a connection to the RADIUS AAA server after the first attempt fails. The default value is 3.

◆ **secret**  
Specifies the shared secret password of the AAA RADIUS server. This option is required.

◆ **timeout**  
Specifies a timeout interval (in seconds) for the AAA RADIUS server after which the server closes a connection. The default value is 5.
◆ use-pool
   Enables or disables the use of the pool specified using the pool option.
   The default value is none.

See also

apm, create, delete, edit, list, modify, show, tmsh
securid

Manages an RSA SecurID authentication server.

Module

apm aaa

Syntax

Configure the securid component within the aaa module using the syntax shown in the following sections.

Create/Modify

create securid [name]
modify securid [name]
  
options:
    config-files [string] | none
    description [string] | none
    source-ip [ip addr]
edit securid | [glob] | [regex] ] ... ]
  
options:
    all-properties
    non-default-properties

Display

list securid
list securid [ [name] | [glob] | [regex] ] ... ]
show running-config securid
show running-config securid [ [name] | [glob] | [regex] ] ... ]
  
options:
    all-properties
    app-service
    non-default-properties
    one-line
    partition
show securid
show securid [name]

Delete

delete securid [name]
Chapter 6

Description

You can use the securid component to create and manage an RSA SecurID authentication server.

Examples

Creates the mySecuridServer AAA RSA SecurID server:

```bash
create securid mySecuridServer {
    config-files add {
        sdconf.rec {
            local-path /shared/tmp/1
        }
    }
    source-ip 172.31.54.138
}
```

Displays a list of AAA RSA SecurID servers on the system:
```
list securid all
```

Deletes the mySecuridServer AAA RSA SecurID server from the system:
```
delete securid mySecuridServer
```

Options

You can use these options with the securid component:

- **config-files**
  Specifies which files to use for SecurID authentication. Upload a copy of the sdconf.rec file from your RSA Authentication Manager server.

- **description**
  Specifies a description for the configuration file you are uploading.

- **source-ip**
  Specifies the source IP address of the RSA SecurID agent. This option is required when authenticating to the RSA Authentication Manager server.

- **partition**
  Displays the partition within which the component resides.

See also

apm, create, delete, edit, list, modify, show, tmsh
tacacs

Configures a TACACS+ server for implementing client authentication using TACAS+ remotely.

Module

apm aaa

Syntax

Configure the radius component within the aaa module using the syntax shown in the following sections.

Create/Modify

create tacacs
modify tacacs

options:
  address [ip addr]
  auth-service [arap | enable | fwproxy | login | nasi | none | ppp | pt | rcmd | x25]
  auth-type [arap | ascii | chap | mschap | pap]
  description [string] | none
  encrypt [enabled | disabled]
  pool [string] | none
  port [string] | none
  priv-lvl [max | min | user]
  protocol [atalk | deccp | ftp | http | ip | ipx | lat | lcp | osicp | pad | rlogin | telnet | tn3270 | unknown | vines | vpdn | xremote]
  secret [string] | none
  service [arap | connection | firewall | ppp | shell | slip | system | tty-daemon]
  use-pool [string] | none

edit tacacs | [glob] | [regex] ] ... ]

options:
  all-properties
  non-default-properties

Display

list tacacs
list tacacs [ [ [name] | [glob] | [regex] ] ... ]
show running-config tacacs
show running-config tacacs [ [ [name] | [glob] | [regex] ] ... ]

options:
  all-properties
app-service
non-default-properties
one-line
partition
show tacacs
show tacacs [name]

Delete

delete tacacs [name]

Description

You can use the tacacsplus component to create and manage a TACACS+ authentication server.

Examples

Creates a TACACS server named mytacacs with encryption enabled:
create tacacs mytacacs auth-service enable encrypt enabled

Options

You can use these options with the tacacs component:

- **address**
  Specifies the IP address of the TACACS+ server. This option is required.

- **auth-service**
  Specifies the name of the service that the user is requesting to be authenticated to use. This enables the TACACS+ server to behave differently for different types of authentication requests. This option is required.

- **auth-type**
  Specifies the type of authentication to be used for authenticating the user.

- **description**
  Specifies a unique description for the component. The default value is none.

- **encrypt**
  Enables or disables encryption of TACACS+ packets. Recommended for normal use. The default value is enabled.

- **name**
  Specifies the name of an AAA TACACS+ server. This option is required.

- **partition**
  Displays the partition within which the component resides.
pool
Specifies the name of the pool to which this server belongs. The default value is \texttt{none}.

port
Specifies the port number of the server. The default value is \texttt{49}.

priv-lvl
Specifies the privilege level at which the user is authenticating.
   The options are:
   - \texttt{max}
   - \texttt{min}
     This is the default.
   - \texttt{user}

protocol
Specifies the protocol associated with the value specified in the service option, which is a subset of the associated service being used for client authorization or system accounting. The default value is \texttt{unknown}.

secret
Sets the secret key used to encrypt and decrypt packets sent or received from the server. This option is required.

service

use-pool
Enables or disables the use of the pool specified using the \texttt{pool} option. The default value is \texttt{none}.

See also

apm, create, delete, edit, list, modify, show, tmsh
apm epsec Module Components

- Introducing the apm epsec module
- Alphabetical list of components
Introducing the apm epsec module

You can use the `tmsh` components that reside within the `apm epsec` module to configure BIG-IP® Access Policy Manager®. For more information about the `tmsh` hierarchical structure, see Chapter 2, *Understanding and Using the Traffic Management Shell*.

Alphabetical list of components

The remainder of this chapter lists the `tmsh` components that are available in the `apm epsec` module.
epsec-package

Manages an EPSEC package.

Module

apm epsec

Syntax

Configure the epsec-package component within the apm epsec module using the syntax shown in the following sections.

Create

create epsec-package
  options:
    local-path [string]
    server [[string] | none]

Display

list epsec-package
  options:
    all-properties
    non-default-properties
list epsec-package [name]

Install

install epsec-package [name]
  options:
    device-group [string]

Delete

delete epsec-package [name]

Description

You can use the epsec-package component to create, install and manage an EPSEC package.
Examples

- **create epsec-package my_epsec_package local-path /tmp/my_epsec_package**
  Creates an EPSEC package named `my_epsec_package`.

- **list epsec-package**
  Displays a list of EPSEC packages.

- **install epsec-package my_epsec_package**
  Installs the EPSEC package named `my_epsec_package` on this device.

- **install epsec-package my_epsec_package device-group /Common/my_epsec_dg**
  Installs the EPSEC package named `my_epsec_package` on the devices in the device group `/Common/my_epsec_dg`.

- **delete epsec-package my_epsec_package**
  Deletes the EPSEC package named `my_epsec_package`.

Options

- **[name]**
  Specifies the name of the component. This option is required.

- **local-path**
  Specifies the local path of the package to be uploaded. This option is valid only with CREATE command and is a required option.

- **device-group**
  Specifies the device group on which the package will be installed. This option is valid only with INSTALL command.
software-status

Displays the status of the OPSWAT Endpoint Security (EPSEC) software installation.

Module

apm epsec

Syntax

Displays information about the software-status component within the apm epsec module using the following syntax.

Display

show software-status

Description

You can use the software-status component to display the status of the EPSEC software installation, including the version of the EPSEC package being installed and the OESIS software version.

Examples

Displays the status of the EPSEC software installation in a table:

show software-status

See also

create, delete, display, epsec-package, install, list, tmsh
apm policy Module Components

- Introducing the apm policy module
- Alphabetical list of components
Introducing the apm policy module

You can use the tmsh components that reside within the apm policy module to configure BIG-IP® Access Policy Manager®. For more information about the tmsh hierarchical structure, see Chapter 2, Understanding and Using the Traffic Management Shell.

Alphabetical list of components

The remainder of this chapter lists the tmsh components that are available in the apm policy module.
access-policy

Manages an access policy.

Module

apm policy

Syntax

WARNING
F5 Networks® recommends that you do not use the command-line interface to create and manage access policies. Instead, use the Visual Policy editor in the Configuration utility.

See also

apm, create, delete, edit, list, modify, show, tmsh
customization-group

Manages a customization group.

Module

apm policy

Syntax

⚠️ WARNING

F5 Networks recommends that you use the Configuration utility to create and manage customization groups.

See also

agent, profile
image-file

Manages a file that contains an image.

Module

apm policy

Syntax

WARNING

F5 Networks recommends that you use the Configuration utility to create and manage image files.

See also

agent, profile
policy-item

Manages an access policy item.

Module

apm policy

Syntax

⚠️ WARNING

*F5 Networks recommends that you use the Visual Policy editor in the Configuration utility to create and manage access policy items.*

See also

policy
windows-group-policy-file

Manages FullArmor GPAnywhere Windows® group policy files.

Module

apm policy

Syntax

⚠️ WARNING

F5 Networks recommends that you use the Visual Policy editor in the Configuration utility to create and manage FullArmor GPAnywhere Windows group policy files.

See also

policy
9

apm policy agent Module Components

• Introducing the apm policy agent module

• Alphabetical list of components
Introducing the apm policy agent module

You can use the tmsh components that reside within the apm policy agent module to configure BIG-IP® Access Policy Manager®. For more information about the tmsh hierarchical structure, see Chapter 2, Understanding and Using the Traffic Management Shell.

Alphabetical list of components

The remainder of this chapter lists the tmsh components that are available in the apm policy agent module.
aaa-active-directory

Manages an AAA Active Directory® agent.

Module

apm policy agent

Syntax

Configure the `aaa-active-directory` component within the `policy agent` module using the following syntax.

Create/Modify

create aaa-active-directory [name]
modify aaa-active-directory [name]

options
  auth-max-logon-attempt [integer]
  fetch-nested-groups [true | false]
  fetch-primary-groups [true | false]
  hints [true | false]
  query-attrname [[string] | none]
  query-filter [[string] | none]
  server [[string] | none]
  show-extended-error [true | false]
  type [query | auth | last]
  upn [true | false]

Display

list aaa-ldap
list aaa-ldap [ [ [name] | [glob] | [regex] ] ... ]
show running-config aaa-ldap
show running-config aaa-ldap [ [ [name] | [glob] | [regex] ] ... ]

options:
  all
  all-properties
  current-module
  non-default-properties
  one-line
  app-service
  partition
Delete

```
delete aaa-active-directory ([name] | all)
```

Description

You can use the `aaa-active-directory` component to configure an AAA Active Directory agent.

Examples

Creates the query type AAA Active Directory agent named 
`MyADQueryagent` that uses the `be` 
sAMAccountName=%{session.logon.last.username}) filter and the `companyAD` AAA AD Server:

```
create aaa-active-directory MyADQueryagent
    {query-filter "(be sAMAccountName=%{session.logon.last.username})"
        type query
        server "companyAD"
    }
```

Creates the authorization type AAA Active Directory agent named 
`MyADAuthagent` that uses the companyAD AAA AD server:

```
create agent aaa active MyADAuthagent {
    type auth
    server "companyAD"
}
```

Displays a list of AAA Active Directory agents and their properties:

```
list aaa-active-directory all
```

Deletes the `MyADagent` AAA Active Directory agent:

```
delete aaa-active-directory MyADagent
```

Options

You can use these options with the `aaa-active-directory` component:

- **auth-max-logon-attempt**
  
  Specifies the maximum number of opportunities that users have to re-enter credentials after their first attempt to log in fails. If you set this value to a number from 2 to 5 inclusive, the system allows users the specified number of opportunities to log in after the first attempt to log in fails. If you set the value to 1, the system does not allow a second log in opportunity after a first log in attempt fails. The default value is 3.
◆ fetch-nested-groups
When enabled, the system administrator can retrieve the full list of groups that user belongs to, even if the retrieval privileges are nested through other groups to which the user belongs to directly. The default value is false.

◆ fetch-primary-groups
When enabled, the system administrator can retrieve the primary group of a user, and use that name as a group in access policy item rules. The default value is false.

◆ hints
When enabled, the system offers the user an option to create a hint that assists in remembering a password. The default value is false.

◆ query-attnname
Specifies the attribute name that you are adding or deleting for the agent.

◆ query-filter
Specifies the search criteria the system uses when querying an AAA Active Directory server for authentication information. The system supports session variables as part of the search query string.

◆ name
Specifies the name of an AAA Active Directory agent. This setting is required.

◆ partition
Displays the partition within which the component resides.

◆ server
Specifies an AAA Active Directory server that the system uses for Active Directory queries and authentication.

◆ show-extended-error
Specifies to display a verbose error message. The default value is false.

◆ type
Specifies the type of AAA Active Directory agent. The default value is last.

The options are:
  • query
    Specifies that the agent makes a query against the AAA Active Directory Server to retrieve information in accordance with the query-filter and query-attributes options.
  • auth
    Specifies that the agent is an authentication agent only. It uses the AAA Active Directory Server, but only for authentication purposes. APM™ does not get any information from the Domain.
  • last
  • upn
When enabled, APM supports the user principal name (UPN) naming style. Some examples of UPNs are: user@fqdn.of.domain.com, user@upnsuffix.com, and user@domain. The default value is false.
See also

apm, create, delete, edit, list, modify, show, tmsh
aaa-client-cert

Manages an AAA Client Certification agent.

Module

apm policy-agent

Syntax

Configure the aaa-client-cert component within the policy-agent module using the following syntax.

Create/Modify

creamodify aaa-client-cert [name]
create aaa-client-cert [name]
options:
    mode [request | require]

Display

list aaa-client-cert
list aaa-client-cert [ [name] | [glob] | [regex] ] ...
show running-config aaa-client-cert
show running-config aaa-client-cert [ [name] | [glob] | [regex] ] ...
options:
    all
    all-properties
    current-module
    non-default-properties
    one-line
    app-service
    partition

Delete

delete aaa-client-cert [name]

Description

You can use the aaa-client-cert component to configure an AAA Client Certification agent.
Examples

Creates the AAA Client Certification agent named **MyCCagent** in the Common partition:

```
create aaa-client-cert MyCCagent
```

Displays a list of AAA Client Certification agents:

```
list aaa-client-cert all
```

Deletes the **MyCCagent** AAA Client Certification agent:

```
delete aaa-client-cert MyCCagent
```

Options

You can use these options with the **aaa-client-cert** component:

- **name**
  Specifies the name of an AAA client cert agent. This setting is required.

- **mode**
  Specifies the mode (request/require) for this certificate.
  The options are:
  - **request**
    Specifies that the system requests a valid certificate from a client, but always authenticates the client.
  - **require**
    Specifies that the system requires a client to present a valid certificate.

- **partition**
  Displays the partition within which the component resides.

See also

- `apm`, `create`, `delete`, `edit`, `list`, `modify`, `show`, `tmsh`
aaa-crldp

Manages an AAA Certificate Revocation List Distribution Point (CRLDP) agent.

Module

apm policy agent

Syntax

Configure the aaa-crldp component within the policy agent module using the following syntax.

Create/Modify

create aaa-crldp [name]
modify aaa-crldp [name]
    options:
    server (<string> | none)

Display

list aaa-crldp
list aaa-crldp [ [name] | [glob] | [regex] ] ...
show running-config aaa-crldp
show running-config aaa-crldp [ [name] | [glob] | [regex] ] ...
    options:
    all
    all-properties
    app-service
    current-module
    non-default-properties
    one-line
    partition

Delete

delete aaa-crldp [name]

Description

You can use the aaa-crldp component to create and manage an AAA CRLDP agent.
Examples

Creates an AAA CRLDP agent named **MyCCagent** in the Common partition:

```
create aaa-crldp MyCCagent
```

Displays a list of AAA CRLDP agents.

```
list aaa-crldp all
```

Deletes the **MyCCagent** AAA CRLDP agent:

```
delete aaa-crldp MyCCagent
```

Options

You can use these options with the **aaa-crldp** component:

- **name**
  Specifies the name of an agent that you want to display or delete. This setting is required.

- **partition**
  Displays the partition within which the component resides.

- **server**
  Specifies the name of the server on which this agent resides. This option is required.

See also

```
apm, create, delete, edit, list, modify, show, tmsh
```
aaa-http

Manages an AAA HTTP agent.

Module

apm policy-agent

Syntax

Configure the aaa-http component within the policy agent module using the following syntax.

Create/Modify

create aaa-http [name]
modify aaa-http [name]
options
  max-logon-attempt [integer]
  server [[string] | none]

Display

list aaa-http
list aaa-http [ [ [name] | [glob] | [regex] ] ... ]
show running-config aaa-http
show running-config aaa-http [ [ [name] | [glob] | [regex] ] ... ]
options:
  all
  all-properties
  current-module
  non-default-properties
  one-line
  app-service
  partition

Delete

delete aaa-http [name]

Description

You can use the aaa-http component to configure an AAA HTTP agent.
Examples

Creates the aaa-http agent named **MyCCagent** in the Common partition:

```
create aaa-http MyCCagent
```

Displays a list of aaa-http agents:

```
list all aaa-http
```

Deletes the **MyCCagent** aaa-http agent:

```
delete aaa-http MyCCagent
```

Options

You can use these options with the **aaa-http** component:

- **max-logon-attempt**
  Specifies the maximum number of opportunities that users have to re-enter credentials after their first attempt to log in fails. If you set this value to a number from 2 to 5 inclusive, the system allows users the specified number of opportunities to log in after the first attempt to log in fails. If you set the value to 1, the system does not allow a second log in opportunity after a first log in attempt fails. The default value is 3.

- **name**
  Specifies the name of an AAA HTTP agent. This setting is required.

- **partition**
  Displays the partition within which the component resides.

- **server**
  Specifies which AAA HTTP server the system uses for Active Directory queries and authentication.

See also

```
apm, create, delete, edit, list, modify, show, tmsh
```
aaa-ldap

Manages an AAA LDAP agent.

Module

apm policy agent

Syntax

Configure the aaa-ldap component within the policy agent module using the following syntax.

Create/Modify

create aaa-ldap [name]
modify aaa-ldap [name]

options:
   attr-name (<string list> | none) [add | delete]
   fetch-nested-groups [enable | disable]
   filter [[string] | none]
   max-logon-attempt [integer]
   search-dn [[string] | none]
   server [[string] | none]
   show-extended-error [true | false]
   type [query | auth | last]
   user-dn [[string] | none]

Display

list aaa-ldap
list aaa-ldap [ [ [name] | [glob] [regex] ] ... ]
show running-config aaa-ldap
show running-config aaa-ldap [ [ [name] | [glob] [regex] ] ... ]

display:
   all
   all-properties
   current-module
   non-default-properties
   one-line
   app-service
   partition
Delete

`delete aaa-ldap [name]`

Description

Use this component to create, modify, display, or delete an AAA LDAP agent.

Examples

Creates the authorization type AAA LDAP agent named `MyLDAPagent` that is associated with the `companyLDAP` server that uses the `cn=%{session.logon.last.username},cn=users,dc=lab,dc=fp,dc=f5net,dc=com` user domain name, the `cn=users,dc=lab,dc=fp,dc=com` search domain, and the `(SAMAccountName=%{{session.logon.last.username})` filter:

```
create aaa-ldap MyLDAPagent {
  user-dn "cn=%{session.logon.last.username},cn=users,dc=lab,dc=fp,dc=com"
  type auth
  server "companyLDAP"
}
```

```
aaa-ldap MyLDAPagent {
  search-dn "cn=users,dc=lab,dc=fp,dc=com"
  filter "(SAMAccountName=%{{session.logon.last.username})"
  type auth
  server "companyLDAP"
}
```

Creates the query type AAA LDAP agent named `MyLDAPagent` that is associated with the `companyLDAP` server that uses the `cn=users,dc=lab,dc=fp,dc=com` search domain and the `(SAMAccountName=%{{session.logon.last.username})` filter:

```
create aaa-ldap MyLDAPagent {
  search-dn "cn=users,dc=lab,dc=fp,dc=com"
  filter "(SAMAccountName=%{{session.logon.last.username})"
  type query
  server "companyLDAP"
}
```

Displays a list of AAA LDAP agents:

```
list aaa-ldap
```

Deletes the `MyLDAPagent` AAA LDAP agent:

```
delete aaa-ldap MyLDAPagent
```
Options

You can use these options with the **aaa-ldap** component:

- **attr-name**
  Adds an attribute name to the agent or deletes an attribute name from the agent.

- **fetch-nested-groups**
  When enabled, the system administrator can retrieve the full list of groups that user belongs to, even if the retrieval privileges are nested through other groups to which the user belongs to directly. The default value is `false`.

- **filter**
  Specifies the LDAP filter that APM uses when querying an AAA LDAP server for authentication information. You must use the filter option with the **search-dn** option.

- **max-logon-attempt**
  Specifies the maximum number of opportunities that users have to re-enter credentials after their first attempt to log in fails. If you set this value to a number from 2 to 5 inclusive, the system allows users the specified number of opportunities to log in after the first attempt to log in fails. If you set the value to 1, the system does not allow a second log in opportunity after a first log in attempt fails. The default value is 3.

- **name**
  Specifies the name of an AAA LDAP agent. This setting is required.

- **partition**
  Displays the partition within which the component resides.

- **search-dn**
  Specifies the base domain name that APM uses for internal LDAP search operations. You must use the **search-dn** option with the **filter** option.

- **server**
  Specifies the AAA LDAP server that the system uses for LDAP queries and authentication.

- **show-extended-error**
  Specifies to display a verbose error message. The default value is `false`.

- **type**
  Specifies a type of AAA LDAP agent. This setting is required. The default value is `last`.

- **user-dn**
  Specifies the fully qualified domain name (FQDN) of the Access Policy Manager. F5 Networks recommends that you specify this value in lower case and without spaces for compatibility with some specific LDAP servers. The specific content of this string depends on your directory layout.

See also

`apm`, `create`, `delete`, `edit`, `list`, `modify`, `show`, `tmsh`
aaa-ocsp

Manages an AAA Online Certificate Status Protocol (OCSP) agent.

Module

apm policy agent

Syntax

Configure the aaa-ocsp component within the policy agent module using the following syntax.

Create/Modify

create aaa-ocsp [name]
modify aaa-ocsp [name]
  options:
    ocsp-responder <string>

Display

list aaa-ocsp
list aaa-ocsp [ [ [name] | [glob] | [regex] ] ... ]
show running-config aaa-ocsp
show running-config aaa-ocsp [ [ [name] | [glob] | [regex] ] ... ]
  options:
    all
    all-properties
    current-module
    non-default-properties
    one-line
    app-service
    partition

Delete

delete aaa-ocsp [name]

Description

Use this command to create, modify, display, or delete an AAA OCSP agent.
Examples

Creates the AAA OCSP agent named MyCCagent in the Common partition:

```
create aaa-ocsp MyCCagent
```

Displays a list of AAA OCSP agents:

```
list aaa-ocsp all
```

Deletes the MyCCagent AAA OCSP agent:

```
delete aaa-ocsp MyCCagent
```

Options

You can use these options with the `aaa-ocsp` component:

- **name**  
  Specifies the name of an agent that you want to display or delete. This setting is required.

- **ocsp-responder**

- **partition**  
  Displays the partition within which the object resides.

See also

`apm, create, delete, edit, list, modify, show, tmsh`
aaa-radius

Manages an AAA RADIUS agent.

Module

apm policy agent

Syntax

Configure the aaa-radius component within the policy agent module using the following syntax.

Create/Modify

create aaa-radius [name]
modify aaa-radius [name]

options:
  max-logon-attempt <number>
  server (<string> | none)
  show-extended-error (true | false)

Display

list aaa-radius
list aaa-radius [ [name] | [glob] | [regex] ] ... ]
show running-config aaa-radius
show running-config aaa-radius [ [name] | [glob] | [regex] ] ... ]

options:
  all
  all-properties
  current-module
  non-default-properties
  one-line
  app-service
  partition

Delete

delete aaa-radius [name]

Description

Use this command to create, modify, display, or delete an AAA RADIUS agent.
Examples

Creates an AAA RADIUS agent named **Myradiusagent** that is associated with the **companyradius** server.

```bash
create aaa-radius Myradiusagent {server "companyradius"}
```

Displays a list of AAA RADIUS agents:

```bash
list aaa-radius
```

Deletes the **Myradiusagent** AAA RADIUS agent:

```bash
delete aaa-radius Myradiusagent
```

Options

You can use these options with the **aaa-radius** component:

- **max-logon-attempt**
  Specifies the maximum number of opportunities that users have to re-enter credentials after their first attempt to log in fails. If you set this value to a number from 2 to 5 inclusive, the system allows users the specified number of opportunities to log in after the first attempt to log in fails. If you set the value to 1, the system does not allow a second log in opportunity after a first log in attempt fails. The default value is 3.

- **name**
  Specifies the name of an AAA RADIUS agent. This setting is required.

- **partition**
  Displays the partition within which the object resides.

- **server**
  Specifies the AAA RADIUS server that the system uses for RADIUS queries and authentication.

- **show-extended-error**
  Specifies to display a verbose error message. The default value is **false**.

See also

- **apm**, **create**, **delete**, **edit**, **list**, **modify**, **show**, **tmsh**
aaa-securid

Manages an AAA Secure ID agent.

Module

apm policy agent

Syntax

Configure the aaa-securid component within the policy agent module using the following syntax.

Create/Modify

create aaa-securid [name]
modify aaa-securid [name]
  options:
  max-logon-attempt [integer]
  server [[string] | none]
  show-extended-error [true | false]
edit aaa-securid | [glob] | [regex] ] ...]
  options:
  all-properties
  non-default-properties

Display

list aaa-securid
list aaa-securid [ [ [name] | [glob] | [regex] ] ... ]
show running-config aaa-securid
show running-config aaa-securid [ [ [name] | [glob] | [regex] ] ... ]
  options:
  all
  all-properties
  current-module
  non-default-properties
  one-line
  app-service
  partition

Delete

delete aaa-securid [name]
Description

You can use the `aaa-securid` component to create and manage an AAA SecurID agent.

Examples

Creates an AAA SecurID agent named `mySecuridAgent` that is associated to AAA RSA Server `rsa1_106`:

```
create aaa-securid mySecuridAgent { server rsa1_106 }
```

Displays a list of AAA SecurID agents.

```
list all aaa-securid
```

Deletes the `MyCCagent` AAA Client Certification agent:

```
delete aaa-securid MyCCagent
```

Options

You can use these options with the `aaa-securid` component:

- **name**
  Specifies the name of an agent that you want to display or delete. This setting is required.

- **partition**
  Displays the partition within which the component resides.

- **max-logon-attempt**
  Specifies the maximum number of opportunities that users have to re-enter credentials after their first attempt to log in fails. If you set this value to a number from 2 to 5 inclusive, the system allows users the specified number of opportunities to log in after the first attempt to log in fails. If you set the value to 1, the system does not allow a second log in opportunity after a first log in attempt fails. The default value is 3.

- **server**
  Specifies the AAA RSA SecurID server that the system uses for LDAP queries and authentication.

- **show-extended-error**
  Specifies to display a verbose error message. The default value is `false`.

See also

`apm`, `create`, `delete`, `edit`, `list`, `modify`, `show`, `tmsh`
acct-radius

Manages an Acct RADIUS agent.

Module

apm policy agent

Syntax

Configure the acct-radius component within the policy agent module using the following syntax.

Create/Modify

create acct-radius [name]
modify acct-radius [name]
  options:
   server [[string] | none]
edit acct-radius | [glob] | [regex] ] ... ]
  options:
   all-properties
   non-default-properties

Display

list acct-radius
list acct-radius [ [ [name] | [glob] | [regex] ] ... ]
show running-config acct-radius
show running-config acct-radius [ [ [name] | [glob] | [regex] ] ... ]
  options:
   all
   all-properties
   current-module
   non-default-properties
   one-line
   app-service
   partition

Delete

delete acct-radius [name]
Description

You can use the acct-radius component to create and manage an Acct RADIUS agent.

Examples

Creates the MyRADIUSagent Acct RADIUS agent that is associated with the MyRADIUS server:

```bash
create acct-radius MyRADIUSagent { server "MyRADIUS" }
```

Displays a list of Acct RADIUS agents and the servers associated with the agents:

```bash
list acct-radius
```

Deletes the MyRADIUSagent Acct RADIUS agent:

```bash
delete acct-radius MyRADIUSagent
```

Options

You can use these options with the acct-radius component:

- **name**
  Specifies the name of an Acct RADIUS server. This setting is required.

- **partition**
  Displays the partition within which the component resides.

- **server**
  Specifies an Acct RADIUS that the system uses for RADIUS queries and authentication. This option is required.

See also

apm, create, delete, edit, list, modify, show, tmsh
acct-tacacsplus

Manages a TACACS+ Account agent.

Module

apm policy agent

Syntax

Configure the acct-tacacsplus component within the policy agent module using the following syntax.

Create/Modify

create acct-tacacsplus [name]
modify acct-tacacsplus [name]
  options
    server [[string] | none]

Display

list acct-tacacsplus
list acct-tacacsplus [ [ name ] | [ glob ] | [ regex ] ] ...
show running-config acct-tacacsplus
show running-config acct-tacacsplus [ [ name ] | [ glob ] | [ regex ] ] ...
  options:
    all
    all-properties
    current-module
    non-default-properties
    app-service
    partition

Delete

delete acct-tacacsplus [name]

Description

You can use the acct-tacacsplus component to configure a TACACS+ Account agent.
Examples

Creates the agent type TACACS+ Account named MyADQueryagent that uses the companyAD server:

create acct-tacacsplus MyADQueryagent { server "companyAD" }

Displays a list of TACACS+ Account agents and the server associated with each agent:

list acct-tacacsplus all

Deletes the MyADagent TACACS+ Account agent:

delete acct-tacacsplus MyADagent

Options

You can use these options with the acct-tacacsplus component:

- **name**
  Specifies the name of a TACACS+ Account agent. This setting is required.

- **partition**
  Displays the partition within which the component resides.

- **server**
  Specifies the TACACS+ Account server that the system uses for queries and authentication.

See also

apm, create, delete, edit, list, modify, show, tmsh
decision-box

Manages a Decision Box agent.

Module

apm policy agent

Syntax

Configure the decision-box component within the policy agent module using the following syntax.

Create/Modify

create decision-box [name]
modify decision-box [name]
  options
    customization-group [name]

Display

list decision-box
list decision-box [ [ [name] | [glob] | [regex] ] ... ]
show running-config decision-box
show running-config decision-box [ [ [name] | [glob] | [regex] ] ... ]

options:
  all
  all-properties
  app-service
  current-module
  non-default-properties
  one-line
  partition

Delete

delete decision-box ([name] | all)

Description

You can use the decision-box component to configure a Decision Box agent.
Examples

Creates the Decision Box agent named MyADQueryagent:
create dynamic-acl MyADQueryagent

Displays a list of Decision Box agents:
list decision-box all

Deletes the MyADAgent Decision Box agent:
delete decision-box MyADAgent

Options

You can use these options with the decision-box component:

- **customization-group**
  Specifies the name of the existing customization group to which the agent belongs.

- **name**
  Specifies the name of an decision-box agent. This setting is required.

- **partition**
  Displays the partition within which the component resides.

See also

apm, create, delete, edit, list, modify, show, tmsh
**dynamic-acl**

Manages a Dynamic ACL agent.

**Module**

`apm policy agent`

**Syntax**

Configure the `dynamic-acl` component within the `policy agent` module using the following syntax.

**Create/Modify**

create dynamic-acl [name]
modify dynamic-acl [name]

options:
entries [ add | delete | modify | none | replace-all-with]

**Display**

list dynamic-acl
list dynamic-acl [ [ [name] | [glob] | [regex] ] ... ]
show running-config dynamic-acl
show running-config dynamic-acl [ [ [name] | [glob] | [regex] ] ... ]

options:
all
all-properties
app-service
current-module
non-default-properties
one-line
partition

**Delete**

delete dynamic-acl [name]

**Description**

You can use the `dynamic-acl` component to create and manage a dynamic access control list (ACL) agent that parse ACL text input with a specified format from a specified session variable, assigns the parsed entry into a
Dynamic ACL object, and assigns it into a current user session. An ACL is a set of restrictions associated with a resource or favorite that defines access for users and groups.

Examples

Creates the Dynamic ACL agent named **MyDynamicAclAgent**:

```plaintext
create dynamic-acl <dynamic-acl-agent-name> { entries <operator> { <index> { acl <DynamicACLentry> [ format [f5 | cisco] ] source <session.variable source> } } }
```

Displays a list of Dynamic ACL agents:

```plaintext
list dynamic-acl
```

Deletes the Dynamic ACL agent named **MyDynamicAclAgent**:

```plaintext
delete dynamic-acl MyDynamicAclAgent
```

Options

You can use these options with the **dynamic-acl** component:

- **entries**
  Specifies the name of the entry to assign this Dynamic ACL.

- **name**
  Specifies the name of the Dynamic ACL agent. This setting is required.

- **partition**
  Displays the partition within which the component resides.

See also

*apm, create, delete, edit, list, modify, show, tmsh*
ending-allow

Manages an Ending Allow agent.

Module

apm policy agent

Syntax

Configure the ending-allow component within the policy agent module using the following syntax.

Create/Modify

create ending-allow [name]
modify ending-allow [name]

Display

list ending-allow
list ending-allow [ [name] | [glob] | [regex] ] ...
show running-config ending-allow
show running-config ending-allow [ [name] | [glob] | [regex] ] ...

options:
  all
  all-properties
  app-service
  current-module
  non-default-properties
  one-line
  partition

Delete

delete ending-allow ([name] | all)

Description

Access policy endings indicate the final outcome of a branch of an access policy. An Allow ending is a successful ending in which the system displays the user’s home page and grants access to a webtop connection.
Examples

Creates the Ending Allow agent named MyEndingAllowAgent:
create ending-allow MyEndingAllowAgent { }

Displays a list of Ending Allow agents:
list ending-allow

Deletes the Ending Allow agent named MyEndingDeniedAgent:
delete ending-allow MyEndingAllowAgent

Options

You can use these options with the ending-allow component:

◆ name
   Specifies the name of an Ending Allow agent. This option is required.

◆ partition
   Displays the partition within which the component resides.

See also

apm, create, delete, edit, list, modify, show, tmsh
ending-deny

Manages an Ending Deny agent.

Module

apm policy agent

Syntax

Configure the ending-deny component within the policy agent module using the following syntax.

Create/Modify

create ending-deny [name]
modify ending-deny [name]
    options
        customization-group [name]

Display

list ending-deny
list ending-deny [ [ [name] | [glob] | [regex] ] ... ]
show running-config ending-deny
show running-config ending-deny [ [ [name] | [glob] | [regex] ] ... ]
    options:
        all
        all-properties
        app-service
        current-module
        non-default-properties
        one-line
        partition

Delete

delete ending-deny ([name] | all)

Description

Access policy endings indicate the final outcome of a branch of an access policy. The Logon Deny ending is the final result of an unsuccessful logon attempt (the failure could be caused by an incorrect logon attempt, a security
requirement incompatibility, or the use of an unsupported device). Upon reaching a Logon Deny ending, the user sees an error message. You can use the ending-deny component to create and manage an Ending Deny agent.

**Examples**

Creates the Ending Deny agent named **MyEndingDenyAgent** that is associated with the **MyLogOffCG** customization group:

```
create ending-deny MyEndingDenyAgent customization-group MyLogOffCG
```

Displays a list of Ending Deny agents:

```
list ending-deny
```

Deletes the Ending Deny agent named **MyEndingDenyAgent**:

```
delete ending-deny MyEndingDenyAgent
```

**Options**

You can use these options with the ending-deny component:

- **customization-group**
  Specifies the name of the existing customization-group to which the agent belongs. It enables you to customize the Logon Deny Page. For example, you can indicate a specific reason for the denial of access. This setting is required, and the customization group that you assign must be of the type **logout**.

- **name**
  Specifies the name of an Ending Deny agent. This setting is required.

- **partition**
  Displays the partition within which the component resides.

**See also**

apm, create, delete, edit, list, modify, show, tmsh
ending-redirect

Manages an Ending Redirect agent.

Module

apm policy agent

Syntax

Configure the ending-redirect component within the policy agent module using the following syntax.

Create/Modify

create ending-redirect [name]
modify ending-redirect [name]
  options
    close-session [true | false]
    url [value]

Display

list ending-redirect
list ending-redirect [ [ [name] | [glob] | [regex] ] ... ]
show running-config ending-redirect
show running-config ending-redirect [ [ [name] | [glob] | [regex] ] ... ]
  options:
    all
    all-properties
    app-service
    current-module
    non-default-properties
    one-line
    partition

Delete

delete ending-redirect ([name] | all)

Description

The Redirect ending can be used to redirect the user, rather than allowing or denying a connection. It can also send a user directly to an update script or to different server or landing URI. Upon reaching a Redirect ending, the
user sees a screen indicating that they are being redirected to a different URL. You can use the `ending-redirect` component to create and manage an Ending Redirect agent.

### Examples

Creates the Ending Redirect agent named `MyEndingRedirectAgent` that redirects a connection to `http://www.myweb.com`:

```
create ending-redirect MyEndingRedirectAgent { url "http://www.myweb.com" }
```

Creates an agent using the current protocol and the session variable `%{sesession.server.network.protocol}`:

```
create ending-redirect MyEndingRedirectAgent { url "%{sesession.server.network.protocol}://www.myweb.com" }
```

Displays a list of Ending Redirect agents

```
list ending-redirect
```

Deletes the Ending Redirect agent named `MyEndingRedirectAgent`:

```
delete ending-redirect MyEndingRedirectAgent
```

### Options

You can use these options with the `ending-redirect` component:

- **close-session**
  Redirects to the specified URI after closing the session if `enabled`. Otherwise, redirect to the specified URI without closing the session. The default value is `enabled`.

- **name**
  Specifies the name of an Ending Redirect agent. This option is required.

- **url**
  Specifies the URL to which the system redirects the original request. This option is required, and you must specify an absolute URL. An absolute URL specifies the exact location of a file or directory on the Internet.

### See also

`apm`, `create`, `delete`, `edit`, `list`, `modify`, `show`, `tmsh`
endpoint-check-av

Manages an Endpoint Check Anti-virus (AV) agent.

Module

apm policy agent

Syntax

Configure the endpoint-check-av component within the policy agent module using the following syntax.

Create/Modify

create endpoint-check-av [name]
modify endpoint-check-av [name]

options:
   items [db-age | db-version | id | state | version ]
edit endpoint-check-av [ [ [name] | [glob] | [regex] ] ... ]

options:
   all-properties
   non-default-properties

Display

list endpoint-check-av
list endpoint-check-av [ [ [name] | [glob] | [regex] ] ... ]
show running-config endpoint-check-av
show running-config endpoint-check-av [ [ [name] | [glob] | [regex] ] ... ]

options:
   all
   all-properties
   app-service
   current-module
   non-default-properties
   one-line
   partition

Delete

delete endpoint-check-av ([name] | all)
Description

Endpoint security is a centrally-managed method of monitoring and maintaining client-system security. You can use the `endpoint-check-av` component to create and manage an agent that enforces anti-virus protection and performs endpoint checks for viruses.

Examples

Creates the Endpoint Check Antivirus agent named `MyEndpointWCAV` agent, which verifies that the specified anti-virus software is running on the client that is attempting to connect:

```
create endpoint-check-av MyEndpointWCAVagent items state enabled add
```

Displays a list of Endpoint Check Anti-virus agents:

```
list endpoint-check-av
```

Deletes the Endpoint Check Anti-virus agent named `MyEndpointWCAV` agent:

```
delete endpoint-check-av MyEndpointWCAVagent
```

Options

You can use these options with the `endpoint-check-av` component:

- **items**
  Adds items to or deletes items from an Endpoint Check AV agent. You can specify the following attributes for the antivirus software:
  - **db-age**
    Specifies the maximum age of the anti-virus database that you want an Endpoint Check AV agent to verify the presence of on the client in order to allow the access policy to pass.
  - **db-version**
    Specifies the version of the anti-virus database that you want an Endpoint Check AV agent to verify the presence of on the client in order to allow the access policy to pass.
  - **id**
    Specifies the ID of the anti-virus software that you want an Endpoint Check AV agent to verify the presence of on the client in order to allow the access policy to pass.
  - **state**
    Specifies whether an Endpoint Check AV agent verifies that the specified anti-virus software is running on the client that is attempting to connect. When disabled, the agent verifies only that the anti-virus software is present on the system. The default value is `disabled`.
• **version**
  Specifies the version of the anti-virus software that you want an
  Endpoint Check AV agent to verify the presence of on the client in
  order to allow the access policy to pass.

  ◆ **[name]**
  Specifies the name of an Endpoint Check AV agent. This option is
  required.

  ◆ **partition**
  Displays the partition within which the component resides.

**See also**

apm, create, delete, edit, list, modify, show, tmsh
endpoint-check-fw

Manages an Endpoint Check Firewall (FW) agent.

Module

apm policy agent

Syntax

Configure the endpoint-check-fw component within the policy agent module using the following syntax.

Create/Modify

create endpoint-check-fw [name]
modify endpoint-check-fw [name]
options
  items [ id | state | version ]
edit endpoint-check-fw [ [ [name] | [glob] | [regex] ] ... ]
options:
  all-properties
  non-default-properties

Display

list endpoint-check-fw
list endpoint-check-fw [ [ [name] | [glob] | [regex] ] ... ]
show running-config endpoint-check-fw
show running-config endpoint-check-fw [ [ [name] | [glob] | [regex] ] ... ]
options:
  all
  all-properties
  app-service
  current-module
  non-default-properties
  one-line
  partition

Delete

delete endpoint-check-fw ([name] | all)
Description

Endpoint security is a centrally-managed method of monitoring and maintaining client-system security. You can use the `endpoint-check-fw` component to create or manage an Endpoint Check FW agent that checks for the presence of the specified firewall on a client.

Examples

Creates the Endpoint Check FW agent named `MyEndpointWCFWagent`, to which you can add items that you want the agent to verify the presence of on the client:

```
create endpoint-check-fw MyEndpointWCFWagent {}  
```

Creates the Endpoint Check FW agent named `MyEndpointWCFWagent`, which verifies that the firewall running on the client that is attempting to connect is version 2.0:

```
create endpoint-check-fw MyEndpointWCFWagent { items state enable version 2.0 }
```

Displays a list of Endpoint Check FW agents:

```
list endpoint-check-fw show
```

Deletes the Endpoint Check FW agent named `MyEndpointWCFWagent`:

```
delete endpoint-check-fw MyEndpointWCFWagent delete
```

Options

You can use these options with the `endpoint-check-fw` component:

- **items**
  Adds an item to or deletes an item from an Endpoint Check FW agent. You can specify the following attributes to define the item:
  - **ID**
    Specifies the version of the firewall that you want an Endpoint Check FW agent to verify on the client in order to allow the access policy to pass.
  - **state**
    Specifies whether an Endpoint Check FW agent verifies that the specified firewall is running on the client that is attempting to connect. When you enable this attribute, you must specify either the ID or version of the firewall for which you want the agent to check. The default value is `disabled`.
  - **version**
    Specifies the version of the firewall that you want an Endpoint Check FW agent to verify on the client in order to allow the access policy to pass.
Chapter 9

- **name**
  Specifies the name of an Endpoint Check FW agent. This setting is required.

- **partition**
  Displays the partition within which the object resides.

**See also**

apm, create, delete, edit, list, modify, show, tmsh
endpoint-linux-check-file

Manages an Endpoint Linux Check File agent.

Module

apm policy agent

Syntax

Configure the endpoint-linux-check-file component within the policy agent module using the following syntax.

Create/Modify

create endpoint-linux-check-file [name]
modify endpoint-linux-check-file [name]
  options:
    files [ filename | md5 | modified | size ]
edit endpoint-linux-check-file [ [ [name] | [glob] | [regex] ] ... ]
  options:
    all-properties
    non-default-properties

Display

list endpoint-linux-check-file
list endpoint-linux-check-file [ [ [name] | [glob] | [regex] ] ... ]
show running-config endpoint-linux-check-file
show running-config endpoint-linux-check-file [ [ [name] | [glob] | [regex] ] ... ]
  options:
    all
    all-properties
    app-service
    current-module
    non-default-properties
    one-line
    partition

Delete

delete endpoint-linux-check-file ([name] | all)
Description

Access Policy Manager® checks for the presence of one or more files on a client that is attempting to connect. If a file with the described properties exists, the action goes to the successful branch. If the file does not exist, or a file exists but one or more properties are not correct, the action goes to the fallback branch. You can use the `endpoint-linux-check-file` component to create or manage an Endpoint Linux Check File agent that verifies the presence of specified Linux files on a client.

Examples

Creates the Endpoint Linux Check File agent named `Myprofile_act_file_check_ag` that checks that the client contains two files located in the `/tmp/demo` directory: a 12 byte file named `demofile` that was modified no later than January 6, 2007 at 10:30 and has an MD5 checksum of `6b61ad518c23650b17e738e1fa2bb04e`, and a 9-byte file named `testfile` that has an MD5 checksum of `f20d9f2072bbeb6691c0f9c5099b01f3`:

```
create endpoint-linux-check-file Myprofile_act_file_check_ag { 
  files { 
    filename "/tmp/demo/demofile"
    md5 "6b61ad518c23650b17e738e1fa2bb04e"
    modified 2007-06-01 10:30:10
    size 12
  }
  { 
    filename "/tmp/demo/testfile"
    md5 "f20d9f2072bbeb6691c0f9c5099b01f3"
    size 9
  }
}
```

Displays information about the Endpoint Linux Check File agent named `Company8profile_act_file_check_ag`:

```
list all endpoint-linux-check-file Company8profile_act_file_check_ag
```

Deletes the `/tmp/demo/demofile` file from the Endpoint Linux Check File agent named `Company8profile_act_file_check_ag`:

```
delete endpoint-linux-check-file Company8profile_act_check_file { files { filename "/tmp/demo/demofile" } }
```

Options

You can use these options with the `endpoint-linux-check` component:
◆ **files**
   Adds files to or deletes files from an Endpoint Linux Check File agent. You can specify the following attributes of the files that you want an Endpoint Linux Check File agent to verify the presence of on the client in order to allow the access policy to pass.

   - **filename**
     Specifies the name of the file and includes the full path. The Endpoint Linux Check File agent that you are creating must be able to verify the file's presence on the client for the access policy to pass. When you add a file to or delete a file from the agent, this setting is required.

   - **md5**
     Specifies the value of an MD5 checksum. The Endpoint Linux Check File agent you are creating must be able to match the checksum on the client for the access policy to pass. The default value is *none*.

   - **modified**
     Specifies the last modified date of the specified file. The Endpoint Linux Check File agent you are creating must verify this date on the client for the access policy to pass. The default value is `1970-01-01 00:00:00`.

   - **size**
     Specifies the size, in bytes, of the specified file. The Endpoint Linux Check File agent you are creating must verify this size on the client for the access policy to pass. The default value is `0`.

   - **name**
     Specifies the name of an Endpoint Linux Check File agent. This setting is required.

   - **partition**
     Displays the partition within which the component resides.

See also

apm, create, delete, edit, list, modify, show, tmsh
endpoint-linux-check-process

Manages an Endpoint Linux Check Process agent.

Module

apm policy agent

Syntax

Configure the endpoint-linux-check-process component within the policy agent module using the following syntax.

Create/Modify

create endpoint-linux-check-process [name]
modify endpoint-linux-check-process [name]

options

expression [ string | none ]

edit endpoint-linux-check-process [ [ [name] | [glob] | [regex] ] ... ]

options:

all-properties
non-default-properties

Display

list endpoint-linux-check-process
list endpoint-linux-check-process [ [ [name] | [glob] | [regex] ] ... ]

show running-config endpoint-linux-check-process
show running-config endpoint-linux-check-process [ [ [name] | [glob] | [regex] ] ... ]

options:

all

all-properties
app-service
current-module
non-default-properties
one-line
partition

Delete

delete endpoint-linux-check-process [name]
Description
You can use the `endpoint-linux-check-process` component to create and manage an Endpoint Linux Check Process agent that collects information about the Linux processes running on the client.

Examples

Creates the Endpoint Linux Check Process agent named `MyEndpointWCPagent` that checks that the client has either bash or top, and Firefox launched:

```
create endpoint-linux-check-process MyEndpointWCPagent { (bash OR top) AND firefox }
```

Displays a list of Endpoint Linux Check Process agents:

```
list endpoint-linux-check-process
```

Deletes the Endpoint Linux Check Process agent named `MyEndpointWCPagent`:

```
delete endpoint-linux-check-process MyEndpointWCPagent
```

Options

You can use these options with the `endpoint-linux-check-process` component:

- **expression**
  Specifies the expression that you want an Endpoint Linux Check Process agent to use to verify the processes that are running on the client to allow the access policy to pass. You can use the following operators: AND, OR, NOT, (and). You can use wildcards in the process name, for example, `navapsvc.*`.

  If the check is successful, the system returns `1`. If the check fails, the system returns `0`. If the expression is incorrect, the system returns `-1`.

- **name**
  Specifies the name of an Endpoint Linux Check Process agent. This setting is required.

- **partition**
  Displays the partition within which the component resides.

See also

```
apm, create, delete, edit, list, modify, show, tmsh
```
endpoint-mac-check-file

Manages an Endpoint Macintosh® Check File agent.

Module

apm policy agent

Syntax

Configure the endpoint-mac-check-file component within the policy agent module using the following syntax.

Create/Modify

create endpoint-mac-check-file [name]
modify endpoint-mac-check-file [name]
options
  files [ filename | md5 | modified | size ]
edit endpoint-mac-check-file [ [ [name] | [glob] | [regex] ] ... ]
options:
  all-properties
  non-default-properties

Display

list endpoint-mac-check-file
list endpoint-mac-check-file [ [ [name] | [glob] | [regex] ] ... ]
show running-config endpoint-mac-check-file
show running-config endpoint-mac-check-file [ [ [name] | [glob] | [regex] ] ... ]
options:
  all
  all-properties
  app-service
  current-module
  non-default-properties
  one-line
  partition

Delete

delete endpoint-mac-check-file ([name] | all)
Description

Access Policy Manager checks for the presence of one or more files on a client that is attempting to connect. If a file with the described properties exists, the action goes to the successful branch. If the file does not exist, or a file exists but one or more properties are not correct, the action goes to the fallback branch. You can use the `endpoint-mac-check-file` component to create or manage an Endpoint Macintosh Check File agent that verifies the presence of specified Macintosh files on a client.

Examples

Creates the Endpoint Macintosh Check File agent named `Myprofile_act_file_check_ag` that checks that the client contains two files located in the `/tmp/demo` directory: a 12 byte file named `demofile` that was modified no later than January 6, 2007 at 10:30 and has an MD5 checksum of `6b61ad518c23650b17e738e1fa2bb04e`, and a 9 byte file named `testfile` that has an MD5 checksum of `f20d9f2072bbeb6691c0f9c5099b01f3`:

```bash
create endpoint-mac-check-file Myprofile_act_file_check_ag {
  files {
    filename "/tmp/demo/demofile"
    md5 "6b61ad518c23650b17e738e1fa2bb04e"
    modified 2007-06-01 10:30:10
    size 12
  }
  {
    filename "/tmp/demo/testfile"
    md5 "f20d9f2072bbeb6691c0f9c5099b01f3"
    size 9
  }
}
```

Displays information about the Endpoint Macintosh Check File agent named `Company8profile_act_file_check_ag`:

```bash
list all endpoint-mac-check-file Company8profile_act_file_check_ag
```

Deletes the `/tmp/demo/demofile` file from the Endpoint Macintosh Check File agent named `Company8profile_act_file_check_ag`:

```bash
delete endpoint-mac-check-file Company8profile_act_file_check_ag { files { filename "/tmp/demo/demofile" } }
```
Options

You can use these options with the `endpoint-mac-check-file` component:

- **files**
  Adds files to or deletes files from an Endpoint Macintosh Check File agent. You can specify the following attributes of the files that you want an Endpoint Macintosh Check File agent to verify the presence of on the client to allow the access policy to pass:
  - **filename**
    Specifies the name of the file and includes the full path. The Endpoint Macintosh Check File agent that you are creating must be able to verify the file’s presence on the client for the access policy to pass. When you add a file to or delete a file from the agent, this setting is required.
  - **md5**
    Specifies the value of an MD5 checksum. The Endpoint Macintosh Check File agent you are creating must be able to match the checksum on the client for the access policy to pass. The default value is `none`.
  - **modified**
    Specifies the last modified date of the specified file. The Endpoint Macintosh Check File agent you are creating must verify this date on the client for the access policy to pass. The default value is `1970-01-01 00:00:00`.
  - **size**
    Specifies the size, in bytes, of the specified file. The Endpoint Macintosh Check File agent you are creating must verify this size on the client for the access policy to pass. The default value is `0`.
- **name**
  Specifies the name of an Endpoint Macintosh Check File agent. This setting is required.
- **partition**
  Displays the partition within which the component resides.

See also

`apm, create, delete, edit, list, modify, show, tmsh`
endpoint-mac-check-process

Manages an Endpoint Macintosh Check Process agent.

Module

apm policy agent

Syntax

Configure the endpoint-mac-check-process component within the policy agent module using the following syntax.

Create/Modify

create endpoint-mac-check-process [name]
modify endpoint-mac-check-process [name]
options
expression [ string | none ]
edit endpoint-mac-check-process [ [ [name] | [glob] | [regex] ] ... ]
options:
  all-properties
  non-default-properties

Display

list endpoint-mac-check-process
list endpoint-mac-check-process [ [ [name] | [glob] | [regex] ] ... ]
show running-config endpoint-mac-check-process
show running-config endpoint-mac-check-process [ [ [name] | [glob] | [regex] ] ... ]
options:
  all
  all-properties
  app-service
  current-module
  non-default-properties
  one-line
  partition

Delete

delete endpoint-mac-check-process ([name] | all)
Description

You can use the `endpoint-mac-check-process` component to create and manage an Endpoint Macintosh Check Process agent that collects information about the Macintosh processes running on the client.

Examples

Creates the Endpoint Macintosh Check Process agent named `MyEndpointWCPagent` that checks that the client has either bash or top, and Firefox launched:

```
create endpoint-mac-check-process MyEndpointWCPagent { (bash OR top) AND firefox }
```

Displays a list of Endpoint Macintosh Check Process agents:

```
list endpoint-mac-check-process
```

Deletes the Endpoint Macintosh Check Process agent named `MyEndpointWCPagent`:

```
delete endpoint-mac-check-process MyEndpointWCPagent
```

Options

You can use these options with the `endpoint-mac-check-process` component:

- **expression**
  Specifies the expression that you want an Endpoint Macintosh Check Process agent to use to verify the processes that are running on the client in order to allow the access policy to pass. You can use the following operators: AND, OR, NOT, (and). You can use wildcards in the process name, for example, `navapsvc.*`.

  If the check is successful, the system returns `1`. If the check fails, the system returns `0`. If the expression is incorrect, the system returns `-1`.

- **name**
  Specifies the name of an Endpoint Macintosh Check Process agent. This setting is required.

- **partition**
  Displays the partition within which the component resides.

See also

`apm`, `create`, `delete`, `edit`, `list`, `modify`, `show`, `tmsh`
endpoint-windows-browser-cache-cleaner

Manages an Endpoint Windows® Browser Cache Cleaner agent.

**Module**

apm policy agent

**Syntax**

Configure the **endpoint-windows-browser-cache-cleaner** component within the **policy agent** module using the following syntax.

**Create/Modify**

```
create endpoint-windows-browser-cache-cleaner [name]
modify endpoint-windows-browser-cache-cleaner [name]
```

**options**

```
cache-clean-type [all | all-except-css-js | all-except-img-css-js | none ]
clean-passwords [false | true ]
empty-recycle-bin [false | true ]
idle-timeout [<integer> | immediate | indefinite]
idle-timeout-screen-lock [<integer>]
monitor-webtop [enable | disable]
partition <name>
    remove-connection-entry [false | true ]
```

**edit endpoint-windows-browser-cache-cleaner** [ [ [name] | [glob] | [regex] ] ... ]

**options:**

```
all-properties
non-default-properties
```

**Display**

```
list endpoint-windows-browser-cache-cleaner
list endpoint-windows-browser-cache-cleaner  [ [ [name] | [glob] | [regex] ] ... ]
show running-config endpoint-windows-browser-cache-cleaner
show running-config endpoint-windows-browser-cache-cleaner  [ [ [name] | [glob] | [regex] ] ... ]
```

**options:**

```
all
all-properties
app-service
current-module
```
Delete

\[
dele\te \text{endpoint-windows-browser-cache-cleaner} \ \ ([\text{name}] \ | \ \text{all})
\]

Description

Endpoint security is a centrally-managed method of monitoring and maintaining client-system security. You can use the `endpoint-windows-browser-cache-cleaner` component to create and manage an Endpoint Windows Browser Cache Cleaner agent. This agent cleans items from the client browser and computer after logoff, and also enforces session inactivity timeouts.

Examples

Creates the Endpoint Windows Browser Cache Cleaner agent named `MyEndpointWBCCAgent` that does not enforce a timeout:

\[
\text{create endpoint-windows-browser-cache-cleaner MyEndpointWBCCAgent idle timeout 0}
\]

Creates the Endpoint Windows Browser Cache Cleaner agent named `MyEndpointWBCCAgent` that does not enforce a timeout, but does clear saved passwords from the client after logoff:

\[
\text{create endpoint-windows-browser-cache-cleaner MyEndpointWBCCAgent \{ idle timeout 0 clean passwords enable \}}
\]

Displays a list of Endpoint Windows Browser Cache Cleaner agents:

\[
\text{list endpoint-windows-browser-cache-cleaner}
\]

Deletes the Endpoint Windows Browser Cache Cleaner agent named `MyEndpointWBCCAgent`:

\[
\text{delete endpoint-windows-browser-cache-cleaner MyEndpointWBCCAgent}
\]

Options

You can use these options with the `endpoint-windows-browser-cache-cleaner` component:

- **cache-clean-type**
  Specifies which browser cache temporary files are removed. If set to `all`, the temporary files are removed. If set to `all-except-css-js`, the browser cache is cleared, but all style sheets and JavaScript™ are left on the browser cache. If set to `all-except-img-css-js`, the browser cache is cleared, but all style sheets, JavaScript, and images are left on the browser cache. The default value is `all`. 
◆ **clean-passwords**
   When true, the Endpoint Windows Browser Cache Cleaner agent ensures that saved passwords are cleared from the client after logoff. The default value is false.

◆ **empty-recycle-bin**
   When true, the Endpoint Windows Browser Cache Cleaner agent empties the Recycle Bin on the client after logoff. The default value is false.

◆ **idle-timeout**
   Specifies the number of minutes that the client session can be idle before the Endpoint Windows Browser Cache Cleaner agent disconnects the session. The default value is 0, which enforces no timeout. This is a required setting.

◆ **idle-timeout-screen-lock**
   Specifies the number of minutes the system can receive no user input before the workstation is locked. The default value is 0, which specifies no timeout enforced.

◆ **monitor-webtop**
   When true, the Endpoint Windows Browser Cache Cleaner agent forces session termination if the browser or webtop is closed. The default value is false.

◆ **name**
   Specifies the name of the Endpoint Windows Browser Cache Cleaner agent. This is a required setting.

◆ **partition**
   Displays the partition within which the component resides.

◆ **remove-connection-entry**
   When true, the Endpoint Windows Browser Cache Cleaner agent removes the connection from the Network Connections Dial-up Networking folder on the client. The default value is false.

### See also

apm, create, delete, edit, list, modify, show, tmsh
endpoint-windows-check-file

Manages an Endpoint Windows Check File agent.

Module

apm policy agent

Syntax

Configure the endpoint-windows-check-file component within the policy agent module using the following syntax.

Create/Modify

create endpoint-windows-check-file [name]
modify endpoint-windows-check-file [name]
   options
   files [ filename | md5 | modified | operation | signer | size | version ]
edit endpoint-windows-check-file [ [ [name] | [glob] | [regex] ] ... ]
   options:
   all-properties
   non-default-properties

Display

list endpoint-windows-check-file
list endpoint-windows-check-file [ [ [name] | [glob] | [regex] ] ... ]
show running-config endpoint-windows-check-file
show running-config endpoint-windows-check-file [ [ [name] | [glob] | [regex] ] ... ]
   options:
   all
   all-properties
   app-service
   current-module
   non-default-properties
   one-line
   partition

Delete

delete endpoint-windows-check-file ([name] | all)
Description

Access Policy Manager checks for the presence of one or more files on a client that is attempting to connect. If a file with the described properties exists, the action goes to the successful branch. If the file does not exist, or a file exists but one or more properties are not correct, the action goes to the fallback branch. You can use the `endpoint-windows-check-file` component to create or manage an Endpoint Windows Check File agent that verifies the presence of specified Windows files on a client.

Examples

Creates the Endpoint Windows Check File agent named `Myprofile_act_file_check_ag` that checks that the client contains two files located in the `C:\demo` directory: a 12 byte file named `demofile` that was modified no later than January 6, 2007 at 10:30 and has an MD5 checksum of `6b61ad518c23650b17e738e1fa2bb04e`, and a 9 byte file named `test.file` that has an MD5 checksum of `f20d9f2072bbeb6691c0f9c5099b01f3`:

```
create endpoint-windows-check-file Myprofile_act_file_check_ag
{ files {
    filename "C:\demo\demofile"
    md5 "6b61ad518c23650b17e738e1fa2bb04e"
    modified 2007-06-01 10:30:10
    size 12
}
{ filename "C:\demo\test.file"
    md5 "f20d9f2072bbeb6691c0f9c5099b01f3"
    size 9
}
}
```

Displays information about the Endpoint Windows Check File agent named `Company8profile_act_file_check_ag`:

```
list all endpoint-windows-check-file Company8profile_act_file_check_ag
```

Deletes the `C:\demo\demofile` file from the Endpoint Windows Check File agent named `Company8profile_act_file_check_ag`:

```
delete endpoint-windows-check-file Company8profile_act_check_file { files { filename "C:\demo\demofile" }}
```
Options

You can use these options with the `endpoint-windows-check-file` component:

- **files**
  Adds files to or deletes files from an Endpoint Windows Check File agent. You can specify the following attributes for the files that you want an Endpoint Windows Check File agent to verify the presence of on the client to allow the access policy to pass.
  - **filename**
    Specifies a file name and includes the full path. The Endpoint windows Check File agent you are creating must be able to verify the file's presence on the client for the access policy to pass. When you add a file to or delete a file from the agent, this setting is required.
  - **md5**
    Specifies the value of an MD5 checksum. The Endpoint windows Check File agent that you are creating must match the checksum on the client for the access policy to pass. The default value is `none`.
  - **modified**
    Specifies the last modified date of the specified file. The Endpoint windows Check File agent you are creating must verify this date on the client for the access policy to pass. The default value is `1970-01-01 00:00:00`.
  - **operation**
    Specifies the operator that you want your Endpoint Windows Check File agent to use when verifying the attributes of the specified file on the client. The default value is `equal`.
  - **signer**
    Specifies that the Endpoint Windows Check File agent must verify that the specified file on the client is signed for the access policy to pass. The default value is `none`.
  - **size**
    Specifies the size, in bytes, of the specified file. The Endpoint Windows Check File agent you are creating must verify this file size on the client for the access policy to pass. The default value is `0`.
  - **version**
    Specifies the version of the specified file that you want your Endpoint Windows Check File agent to verify on the client for the access policy to pass. Specify the version using the following form: `x.x.x.x`. The maximum value is `65535.65535.65535.65535`. The default value is `none`.

- **name**
  Specifies the name of an Endpoint Windows Check File agent. This option is required.

- **partition**
  Displays the partition within which the component resides.
See also

apm, create, delete, edit, list, modify, show, tmsh
endpoint-windows-check-machine-cert

Manages an Endpoint Windows Check Machine certificate agent.

Module

apm policy agent

Syntax

Configure the endpoint-windows-check-machine-cert component within the policy agent module using the following syntax.

Create/Modify

create endpoint-windows-check-machine-cert [name]
modify endpoint-windows-check-machine-cert [name]

options:
  ca-profile-name [value]
  issuer [value]
  match-rule [any | issuer | issuer-and-serial-num | last | subject-alt-name-match-fqdn | subject-on-match-fqdn ]
  ocsp-responder-name [value]
  save-cert [ true| false]
  serial-number [integer]
  store-location [machine | user]
  store-name [value]
  subject-alt-name [value]

edit endpoint-windows-check-machine-cert [ [ [name] | [glob] | [regex] ] ... ]

options:
  all-properties
  non-default-properties

Display

list endpoint-windows-check-machine-cert
list endpoint-windows-check-machine-cert [ [name] | [glob] | [regex] ] ... ]
show running-config endpoint-windows-check-machine-cert
show running-config endpoint-windows-check-machine-cert [ [name] | [glob] | [regex] ] ... ]

options:
  all
  all-properties
  app-service
  current-module
Delete

```
delete endpoint-windows-check-machine-cert [name]
```

Description

Endpoint security is a centrally managed method of monitoring and maintaining client-system security. The `endpoint-windows-check-machine-cert` component checks for the presence of a valid machine certificate on Windows client systems during access policy validation.

Examples

Creates the Endpoint Windows Check Machine certificate agent named MyMCagent in the Common partition:

```
create endpoint-windows-check-machine-cert MyMCagent
```

Displays a list of Endpoint Windows Check Machine certificate agents:

```
list endpoint-windows-check-machine-cert
```

Deletes the MyMCagent Endpoint Windows Check Machine certificate agent:

```
delete endpoint-windows-check-machine-cert MyMCagent
```

Options

You can use these options with the `endpoint-windows-check-machine-cert` component:

- **ca-profile-name**
  Specifies the name of the certificate authority profile to validate the certificate.

- **issuer**
  Specifies the name used to match the issuer name in the machine certificate.

- **match-rule**
  Specifies the match rule to look up the machine certificate on the client machine.

- **name**
  Specifies the name of an external logon page agent. This option is required.
◆ **ocsp-responder-name**
   Specifies the name of the OCSP responder to validate the certificate using OCSP.

◆ **partition**
   Displays the partition within which the component resides.

◆ **save-cert**
   Specifies to store the entire machine certificate in a session variable.

◆ **serial-number**
   Specifies the serial-number used to match the serial number of the machine certificate.

◆ **store-location**
   Specifies the location of the certificate store on the client machine.

◆ **store-name**
   Specifies the name of the certificate store on the client machine.

◆ **subject-alt-name**
   Specifies the name used to match the subject-alt-name in the machine certificate.

◆ **partition**
   Specifies the partition within which the object resides.

**See also**

`apm`, `create`, `delete`, `edit`, `list`, `modify`, `show`, `tmsh`
endpoint-windows-check-process

Manages an Endpoint Windows Check Process agent.

Module

apm policy agent

Syntax

Configure the endpoint-windows-check-process component within the policy agent module using the following syntax.

Create/Modify

create endpoint-windows-check-process [name]
modify endpoint-windows-check-process [name]

options:
  expression (<string> | none)
edit endpoint-windows-check-process [ [ [name] | [glob] | [regex] ] ... ]

options:
  all-properties
  non-default-properties

Display

list endpoint-windows-check-process
list endpoint-windows-check-process [ [ [name] | [glob] | [regex] ] ... ]
show running-config endpoint-windows-check-process
show running-config endpoint-windows-check-process [ [ [name] | [glob] | [regex] ] ... ]

options:
  all-properties
  non-default-properties
  partition
show endpoint-windows-check-process
show endpoint-windows-check-process [name]

Delete

delete endpoint-windows-check-process [name]
Description

You can use the `endpoint-windows-check-process` component to create and manage an agent that collects information about the Windows processes running on the client.

Examples

 Creates the Endpoint Windows Check Process agent named `MyEndpointWCPagent` that checks that the client has either NISUM.exe or blackd.exe, and navapsvc.* installed:

```plaintext
create endpoint-windows-check-process MyEndpointWCPagent { (NISUM.exe OR blackd.exe) AND navapsvc.* }
```

 Displays a list of Endpoint Windows Check Process agents:

```plaintext
list endpoint-windows-check-process
```

 Deletes the Endpoint Windows Check Process agent named `MyEndpointWCPagent`:

```plaintext
delete endpoint-windows-check-process MyEndpointWCPagent delete
```

Options

You can use these options with the `endpoint-windows-check-process` component:

- **aexpression**
  Specifies the expression that you want an Endpoint Windows Check Process agent to use to verify the processes that are running on the client in order to allow the access policy to pass. You can use the following operators: AND, OR, NOT, (and).
  You can use wildcards in the process name, for example, navapsvc.*. If the check is successful, the system returns 1. If the check fails, the system returns 0. If the expression is incorrect, the system returns -1.

- **name**
  Specifies the name of an Endpoint Windows Check Process agent. This setting is required.

- **partition**
  Displays the partition within which the component resides.

See also

`apm, create, delete, edit, list, modify, show, tmsh`
**endpoint-windows-check-registry**

Manages an Endpoint Windows Check Registry agent.

**Module**

```
apm policy agent
```

**Syntax**

Configure the `endpoint-windows-check-registry` component within the `policy agent` module using the following syntax.

**Create/Modify**

```
create endpoint-windows-check-registry [name]
modify endpoint-windows-check-registry [name]
```

**options:**

```
expression [[string] | none]
edit endpoint-windows-check-registry [ [ [name] | [glob] | [regex] ] ... ]
```

**options:**

```
all-properties
non-default-properties
```

**Display**

```
list endpoint-windows-check-registry
list endpoint-windows-check-registry [ [ [name] | [glob] | [regex] ] ... ]
show running-config endpoint-windows-check-registry
show running-config endpoint-windows-check-registry [ [ [name] | [glob] | [regex] ] ... ]
```

**options:**

```
all-properties
non-default-properties
partition
```

**Delete**

```
delete endpoint-windows-check-registry [name]
```
Description

You can use the **endpoint-windows-check-registry** component to create and manage an agent that collects information about the Windows registry keys on the client that is attempting to connect.

Examples

Creates the Endpoint Windows Check Registry agent named **MyEndpointWCRagent** that checks the registry on the client for version 5.0.2800.0 of Internet Explorer in the HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft directory:

```bash
create endpoint-windows-check-registry MyEndpointWCRagent
{"HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Version"="5.0.2800.0"}
```

Creates the Endpoint Windows Check Registry agent named **MyEndpointWCRagent** that checks the registry on the client for version 5.0.2800.0 of Internet Explorer in the HKEY_LOCAL_MACHINE64\SOFTWARE\Microsoft directory:

```bash
create endpoint-windows-check-registry MyEndpointWCRagent
{"HKEY_LOCAL_MACHINE64\SOFTWARE\Microsoft\Internet Explorer\Version"="5.0.2800.0"}
```

Note that the registry value **HKEY_LOCAL_MACHINE64** is one of the 32-bit and 64-bit registry keys that you can specify on 64-bit Windows versions.

On 64-bit Windows systems, you can check for registry keys in either the 64-bit registry or the 32-bit registry. To specify the registry to check, append a number to the registry root key name. The following key names are supported:

- HKEY_CURRENT_USER
- HKEY_CURRENT_USER32
- HKEY_CURRENT_USER64
- HKEY_LOCAL_MACHINE
- HKEY_LOCAL_MACHINE32
- HKEY_LOCAL_MACHINE64
- HKEY_CLASSES_ROOT
- HKEY_CLASSES_ROOT32
- HKEY_CLASSES_ROOT64
- HKEY_USERS
- HKEY_USERS32
- HKEY_USERS64

HKEY values specified with a 32 appended allow you to check values in the 32-bit view of 64-bit registry. This is the perspective used by 32-bit applications running with on a 64-bit operating system.
HKEY values with a 64 appended allow you to check values in the 64-bit view of the registry. This is the perspective used by native 64-bit applications. When checking values on 32-bit Windows, the number of bits specified in the registry key name is ignored.

Displays a list of Endpoint Windows Check Registry agents:

```
list endpoint-windows-check-registry
```

Deletes the Endpoint Windows Check Registry agent named **MyEndpointWCRagent**:

```
delete endpoint-windows-check-registry MyEndpointWCRagent
```

### Options

You can use these options with the **endpoint-windows-check-registry** component:

- **expression**
  Specifies the expression that you want an Endpoint Windows Check Registry agent to use to verify the registry entries that are present on the client in order to allow the access policy to pass. You can use the following operators: AND, OR, NOT, (and).
  
  If the check is successful, the system returns **1**. If the check fails, the system returns **0**. If the expression is incorrect, the system returns **-1**.

  **Important:** You must use quotation marks (**""**) around key and value arguments, and in data when the content contains spaces, commas, slashes, tabs, or other delimiters. If quotation marks exist as part of a registry path or value name, you must use quotation marks around those quotation marks.

  **Tip:** The system treats data in the formats "d,d[d][.d]" or "d,d[d][.d]d" (where d is a number) as a version number. The system treats data in the format "mm/dd/yyyy" as a date.

- **name**
  Specifies the name of the an Endpoint Windows Check Registry agent. This option is required.

- **partition**
  Displays the partition within which the component resides.

### See also

```
apm, create, delete, edit, list, modify, show, tmsh
```
**endpoint-windows-group-policy**

Manages an Endpoint Windows Group Policy agent.

**Module**

`apm policy agent`

**Syntax**

Configure the `external-logon-page` component within the `policy agent` module using the following syntax.

**Create/Modify**

```plaintext
create endpoint-windows-group-policy [name]
modify endpoint-windows-group-policy [name]
  options:
    policy-file { [name] }
edit endpoint-windows-group-policy [ [ [name] | [glob] | [regex] ] ... ]
  options:
    all-properties
    non-default-properties
```

**Display**

```plaintext
list endpoint-windows-group-policy
list endpoint-windows-group-policy [ [ [name] | [glob] | [regex] ] ... ]
show running-config endpoint-windows-group-policy
show running-config endpoint-windows-group-policy [ [ [name] | [glob] | [regex] ] ... ]
  options:
    all-properties
    non-default-properties
    partition
show endpoint-windows-group-policy
show endpoint-windows-group-policy [name]
```

**Delete**

```plaintext
delete endpoint-windows-group-policy [name]
```
Description

Endpoint Windows Group Policy agents enable you to apply an Endpoint Windows Group Policy to a client machine and create a result session variable.

Examples

Creates a policy for the Access Policy using the Firewall Settings template:

```
create endpoint-windows-group-policy { Firewall_Settings_Template }
```

Edits the Firewall Settings Template:

```
edit endpoint-windows-group-policy Firewall_Settings_Template
```

Options

You can use these options with the `endpoint-windows-group-policy` component:

- **name**
  Specifies a name for the Endpoint Windows Group Policy agent.

- **partition**
  Displays the partition within which the component resides.

- **policy-file**
  Specifies the group policy template that is applied to the client. This option is required.

See also

```
apm, create, delete, edit, list, modify, show, tmsh
```
endpoint-windows-info-os

Manages an Endpoint Windows Information Operating System agent.

Module

apm policy agent

Syntax

Configure the endpoint-windows-info-os component within the policy agent module using the following syntax.

Create/Modify

create endpoint-windows-info-os [name]
modify endpoint-windows-info-os [name]
edit endpoint-windows-info-os [ [ [name] | [glob] | [regex] ] ... ]
options:
  all-properties
  non-default-properties

Display

list endpoint-windows-info-os
list endpoint-windows-info-os [ [ [name] | [glob] | [regex] ] ... ]
show running-config endpoint-windows-info-os
show running-config endpoint-windows-info-os [ [ [name] | [glob] | [regex] ] ... ]
options:
  all-properties
  non-default-properties
  partition
show endpoint-windows-info-os
show endpoint-windows-info-os [name]

Delete

delete endpoint-windows-info-os [name]

Description

You can use the endpoint-windows-info-os component to create and manage an agent that retrieves information about the Microsoft Windows operating system from the client, such as version and hotfix number.
Examples

Creates the Endpoint Windows Operating System Information agent named MyEndpointWIOSagent:

```
create endpoint-windows-info-os MyEndpointWIOSagent { }
```

Displays a list of Endpoint Windows Operating System Information agents:

```
list endpoint-windows-info-os
```

Deletes the Endpoint Windows Operating System Information agent named MyEndpointWCRagent:

```
delete endpoint-windows-info-os MyEndpointWIOSagent delete
```

Options

You can use these options with the `endpoint-windows-info-os` component:

- **name**
  Specifies the name of an Endpoint Windows Info OS agent. This setting is required.

- **partition**
  Displays the partition within which the component resides.

See also

```
apm, create, delete, edit, list, modify, show, tmsh
```
endpoint-windows-machine-info

Manages an Endpoint Windows Machine Information agent.

Module

apm policy agent

Syntax

Configure the **endpoint-windows-machine-info** component within the **policy agent** module using the following syntax.

### Create/Modify

```plaintext
create endpoint-windows-machine-info [name]
modify endpoint-windows-machine-info [name]
edit endpoint-windows-machine-info [ [ [name] | [glob] | [regex] ] ... ]
  options:
    all-properties
    non-default-properties
    one-line
```

### Display

```plaintext
list endpoint-windows-machine-info
list endpoint-windows-machine-info [ [ [name] | [glob] | [regex] ] ... ]
show running-config endpoint-windows-machine-info
show running-config endpoint-windows-machine-info [ [ [name] | [glob] | [regex] ] ... ]
  options:
    all-properties
    non-default-properties
    partition
show endpoint-windows-machine-info
show endpoint-windows-machine-info [name]
```

### Delete

```plaintext
delete endpoint-windows-machine-info [name]
```

### Description

You can use the **endpoint-windows-machine-info** component to create and manage an agent that collects information about the Windows machine that is attempting to connect.
Options

You can use these options with the endpoint-windows-machine-info component:

- **name**
  Specifies the name of the an Endpoint Windows Check Registry agent.
  This setting is required.

- **partition**
  Displays the partition within which the component resides.

See also

apm, create, delete, edit, list, modify, show, tmsh
**endpoint-windows-protected-workspace**

Manages an Endpoint Windows Protected Workspace agent.

**Module**

`apm policy agent`

**Syntax**

Configure the `endpoint-windows-protected-workspace` component within the `policy agent` module using the following syntax.

**Create/Modify**

```
create endpoint-windows-protected-workspace [name]
modify endpoint-windows-protected-workspace [name]
```

```
options:
  allow-burn-cid [true | false]
  allow-printer-use [true | false]
  allow-user-switch [true | false]
  allowed-network-shares [add | delete | modify | replace-all-with] {
    [[string]]
  }
  close-google-desktop-search [true | false]
  usb-flash-access [all | ironkey | none]
```

```
edit endpoint-windows-protected-workspace ...
```

```
options:
  all-properties
  non-default-properties
```

**Display**

```
list endpoint-windows-protected-workspace ...
list endpoint-windows-protected-workspace ...
```

```
show running-config endpoint-windows-protected-workspace ...
show running-config endpoint-windows-protected-workspace ...
```

```
options:
  all-properties
  non-default-properties
  partition
```

```
show endpoint-windows-protected-workspace
show endpoint-windows-protected-workspace [name]
```
Delete

```
dele te endpoint-windows-protected-workspace [name]
```

Description

You can use the `endpoint-windows-protected-workspace` component to create and manage an agent that enables an administrator to impose limitations on applications running on Windows client machines.

Options

You can use these options with the `endpoint-windows-protected-workspace` component:

- **allow-burn-cid**
  Specifies that the user can burn CDs from within protected workspace. The default value is `false`.

- **allow-printer-use**
  Specifies whether a user can print inside a protected workspace. The default value is `true`.

- **allow-user-switch**
  Specifies whether a user can temporarily switch from a protected workspace. The default value is `true`.

- **allowed-network-shares**
  Specifies a list of Windows network shares to which user has Write access. The default value is `none`.

- **name**
  Specifies the name of the Endpoint Windows Protected Workspace agent. This option is required.

- **partition**
  Displays the partition within which the component resides.

- **usb-flash-access**
  Specifies whether a user has access to a USB port. The default value is `false`.

See also

`apm`, `create`, `delete`, `edit`, `list`, `modify`, `show`, `tmsh`
external-logon-page

Manages an External Logon Page agent.

Module

apm policy agent

Syntax

Configure the external-logon-page component within the policy agent module using the following syntax.

Create/Modify

create external-logon-page [name]
modify external-logon-page [name]
   options:
      split-username [true | false]
      uri [[string]> | none]
edit external-logon-page [ [ [name] | [glob] | [regex] ] ... ]
   options:
      all-properties
      non-default-properties

Display

list external-logon-page
list external-logon-page [ [ [name] | [glob] | [regex] ] ... ]
   options:
      all-properties
      non-default-properties
      partition

Delete

delete external-logon-page [name]

Description

The External Logon Page agent creates an external logon page that redirects the client browser.
Examples

- Creates the External Logon Page agent named MyExternalLogonPageAgent that is associated with the URI MyExternalLogonPageServerURI:
  
  ```
  create external-logon-page MyExternalLogonPageAgent { uri "MyExternalLogonPageServerURI" }
  ```

- Creates the External Logon Page agent named MyExternalLogonPageAgent with a URI of session.my_server_uri:
  
  ```
  create external-logon-page MyExternalLogonPageAgent { uri "%(session.my_server_uri)" }
  ```

- Displays a list of External Logon Page agents:
  
  ```
  list external-logon-page
  ```

- Deletes the External Logon Page agent named MyExternalLogonPageAgent:
  
  ```
  delete external-logon-page MyExternalLogonPageAgent
  ```

Options

You can use these options with the external-logon-page component:

- **name**
  
  Specifies the name of an External Logon Page agent. This option is required.

- **partition**
  
  Displays the partition within which the component resides.

- **split-username**
  
  Specifies whether user’s input is split into username and domain. This option supports UPN style logon ID (userid@domainid) and Windows® Domain User account ID (domainid\userid). The default value is false. Set this to true when you want to store the username and domain separately.

- **uri**
  
  Specifies a predefined configuration that contains several settings that you want the agent to use to configure an External logon page. This option is required.

See also

- `apm`, `create`, `delete`, `edit`, `list`, `modify`, `show`, `tmsh`
irule-event

Manages an iRule Event agent.

Module

apm policy agent

Syntax

Configure the irule-event component within the policy agent module using the syntax shown in the following sections.

Create/Modify

create irule-event [name]
modify irule-event [name]
  options:
    id [[string] | none]
edit irule-event [ [ [name] | [glob] | [regex] ] ... ]
  options:
    all-properties
    non-default-properties

Display

list irule-event
list irule-event [ [ [name] | [glob] | [regex] ] ... ]
show running-config irule-event
show running-config irule-event [ [ [name] | [glob] | [regex] ] ... ]
  options:
    all-properties
    non-default-properties
    partition
show irule-event
show irule-event [name]

Delete

delete irule-event [name]
Description

You can use the `irule-event` component to add a custom Access iRule event to an access policy. This agent enables you to combine access policy execution with iRule execution.

For example, you can retrieve the current agent ID (using an iRule command `ACCESS::policy agent_id`) to determine which of the iRule agents raised the event and then perform some custom logic execution.

Examples

`ACCESS_POLICY_AGENT_EVENT` gathers data containing the users whose last logon was within the last two weeks. Note that you can access session variables and create new session variables inside this event:

```bash
when ACCESS_POLICY_AGENT_EVENT {
  if ({[ACCESS::policy agent_id] eq "lastLogon" }
    { # our limit in seconds set 2weeks 1209600 # diff in 100 nanosecond increments between MS time attribute (year 1601) and start of epoch set offset 11644473600000 set adtime "[ACCESS::session data get session.ad.last.attr.lastLogon]" # convert adtime to milliseconds set millisecs [expr {$adtime / 10000}] # subtract offset set lastlogintime [expr {($millisecs - $offset)}] # convert to seconds because milliseconds for 'now' were negative (maybe vmware issue) set secs [expr {$lastlogintime / 1000}] set now [clock seconds] # finally calculate the difference set diff [expr {($now - $secs)}] log local0. "lastLogon: $diff seconds from current time" if { $diff > $2weeks } { ACCESS::session data set session.custom.lastLogonWithin2Weeks 0 } else { ACCESS::session data set session.custom.lastLogonWithin2Weeks 1 }
  }
}
```

Displays a list of OAM agents:
```
list irule-event all
```

Deletes the iRule Event agent named `my_irule_agent`:
```
delete irule-event my_irule_agent
```

Options

You can use these options with the `irule-event` component:

- **id**
  Specifies the ID of the iRule event. The default value is `none`. You can use the ID to determine which agent caused the `ACCESS_POLICY_AGENT_EVENT`. You can also use the ID to perform different processing inside iRule for different agents.

- **name**
  Specifies the name of the component. This option is required.

- **partition**
  Displays the partition within which the component resides.
See also

apm, create, delete, edit, list, modify, show, tmsh
kerberos

Manages a Kerberos agent.

Module

apm policy agent

Syntax

Configure the kerberos component within the policy agent module using the syntax shown in the following sections.

Create/Modify

create kerberos [name]
modify kerberos [name]
  options:
    max-logon-attempt [integer]
    server [string]
edit kerberos [ [ [name] | [glob] | [regex] ] ... ]
  options:
    all-properties
    non-default-properties

Display

list kerberos
list kerberos [ [ [name] | [glob] | [regex] ] ... ]
show running-config kerberos
show running-config kerberos [ [ [name] | [glob] | [regex] ] ... ]
  options:
    all-properties
    non-default-properties
    partition
show kerberos
show kerberos [name]

Delete

delete kerberos [name]
Description

You can use the `kerberos` component to create and manage a Kerberos agent.

Examples

Creates a Kerberos agent named `my_kerberos_agent`:

```
create kerberos my_kerberos_agent
```

Displays a list of Kerberos agents:

```
list kerberos all
```

Deletes the Kerberos agent named `my_kerberos_agent`:

```
delete kerberos my_kerberos_agent
```

Options

You can use these options with the `kerberos` component:

- **name**
  Specifies the name of the component. This option is required.
- **max-logon-attempt**
  Specifies the maximum number of opportunities that users have to re-enter credentials after their first attempt to log in fails. If you set this value to a number from 2 to 5 inclusive, the system allows users the specified number of opportunities to log in after the first attempt to log in fails. If you set the value to 1, the system does not allow a second log in opportunity after a first log in attempt fails. The default value is 3.
- **partition**
  Displays the partition within which the component resides.
- **server**
  Specifies the name of the Kerberos server. This option is required.

See also

`apm`, `create`, `delete`, `edit`, `list`, `modify`, `show`, `tmsh`
logging

Manages a Logging agent.

Module

apm policy agent

Syntax

Configure the logging component within the policy agent module using the syntax shown in the following sections.

Create/Modify

create logging [name]
multiply logging [name]

options:
  log-message [string] | none
  variables [string] | none
edit logging [ [name] | [glob] | [regex] ] ...

options:
  all-properties
  non-default-properties

Display

list logging
list logging [ [name] | [glob] | [regex] ] ...
show running-config logging
show running-config logging [ [name] | [glob] | [regex] ] ...

options:
  all-properties
  app-service
  log-message
  non-default-properties
  partition
  variables

Delete

delete logging [name]
Description

You can use the **logging** component to create and manage a logging agent that monitors the value of session variables and identifies the path taken by access policy execution. A logging agent can also be used to create and monitor custom or predefined session variables. Note that a session variable may or may not exist depending on the result of the access policy execution.

Examples

Creates the logging agent named **MyProfile_act_logging_ag** in partition **Common** and adds two session variables that define actions that the agent logs: 

- **session.logon.** indicates to log application logon attempts and
- **session.windows_check_file.Company8profile_act_file_check_ag.item_x.filename** indicates to log the outcome of the file check on the client. The *x* in item_\_x indicates the order of the files in the list configured for the file checker. The list starts with index **0** (zero):

```plaintext
create logging MyProfile_act_logging_ag { variables { { session-var "session.logon.*" } { session-var "session.windows_check_file.Company8profile_act_file_check_ag.item_x.filename" } } }
```

Displays a list of logging agents:

```plaintext
list logging
```

Options

You can use these options with the **logging** component:

- **app-service**
  
  The default value is **none**.

- **log-message**
  
  Specifies the log message to display. This option is required.

- **name**
  
  Specifies the name of a logging agent. This option is required.

- **partition**
  
  Displays the partition within which the component resides.

- **variables**
  
  Adds a variable to or deletes a variable from a logging agent. You use the **sessionvar** option to specify a session variable that indicates what actions the system logs.

See also

- **apm**, **create**, **delete**, **edit**, **list**, **modify**, **show**, **tmsh**
## logon-page

Manages a Logon Page agent.

### Module

**apm policy agent**

### Syntax

Configure the **logon-page** component within the **policy agent** module using the following syntax.

#### Create/Modify

```
create logon-page [name]
modify logon-page [name]
```

**options:**

```
basic-auth-realm [[string] | none]
customization-group [[string] | none]
field-modifiable1 [true | false]
field-modifiable2 [true | false]
field-modifiable3 [true | false]
field-modifiable4 [true | false]
field-modifiable5 [true | false]
field-type1 [checkbox | none | password | text]
field-type2 [checkbox | none | password | text]
field-type3 [checkbox | none | password | text]
field-type4 [checkbox | none | password | text]
field-type5 [checkbox | none | password | text]
http-401-auth-level [basic | basic-negotiate | negotiate | none]
post-var-name1 [[integer] | none]
post-var-name2 [[integer] | none]
post-var-name3 [[integer] | none]
post-var-name4 [[integer] | none]
post-var-name5 [[integer] | none]
session-var-name1 [[integer] | none]
session-var-name2 [[integer] | none]
session-var-name3 [[integer] | none]
session-var-name4 [[integer] | none]
session-var-name5 [[integer] | none]
split-username [true | false]
type [401 | form-based]
```
edit logon-page [ [ [name] | [glob] | [regex] ] ... ]
  options:
    all-properties
    non-default-properties

Display

list logon-page
list logon-page [ [ [name] | [glob] | [regex] ] ... ]
show running-config logon-page
show running-config logon-page [ [ [name] | [glob] | [regex] ] ... ]
  options:
    all-properties
    non-default-properties
    partition
show logon-page
show logon-page [name]

Delete

delete logon-page [name]

Description

You can use the logon-page component to create and manage a Logon Page agent. This agent creates a logon page that includes the form in which users input the credentials required by an access policy. You can use the customization-group option to customize the logon page.

Examples

Creates a basic authentication Logon Page agent named MyLogonPageAgent that results in a 401 response:
create logon-page MyLogonPageAgent my {
    type 401
    basic-auth-realm myrealm
    split-username false
    http-401-auth-level none
}

Displays a list of Logon Page agents.
list logon-page

Deletes the Logon Page agent named MyLogonPageAgent:
delete logon-page MyLogonPageAgent
Options

You can use these options with the `logon-page` component:

- **basic-auth-realm**
  Specifies the system being accessed for HTTP basic authentication. This value is shown in the 401 response. Use this option only for basic authentication logon pages.

- **customization-group**
  Specifies a predefined configuration that contains several settings that you want the agent to use to configure a logon page. This setting is required, and the customization group that you assign must be of the type `logon`. Use this option only for basic authentication logon pages.

- **field-modifiable1 - field-modifiable5**
  Specifies whether the user can modify the contents of the field on a form-based logon page. The default value is `true`. You can use this option to display read-only information. A logon page can have a maximum of five fields. Use this option only for form-based logon pages.

- **field-type1 - field-type5**
  Specifies the type of fields on a form-based logon page. The default value is `text`. Use this option only for form-based logon pages.

  The options are:

  - checkbox
  - none
  - password
  - text

- **http-401-auth-level**
  Use this option only for basic authentication logon pages.

  The options are:

  - basic
  - basic-negotiate
  - negotiate
  - none

- **name**
  Specifies the name of a Logon Page agent. This setting is required.

- **partition**
  Displays the partition within which the component resides.

- **post-var-name1 - post-var-name5**
  Specifies the name of the variable that is sent with POST request. Use this option only for form-based logon pages.

- **sess-var-name1 - sess-var-name5**
  Specifies the session variable from which the initial value is taken. Use this option only for form-based logon pages.
• **split-username**
  Specifies whether the user's input is split into username and domain. This option supports UPN style logon ID (userid@domainid) and Windows Domain User account ID (domainid\userid). The default value is **false**.
  Set this to true when you want to store the username and domain separately.
  Use this option only for basic authentication logon pages.

• **type**
  Specifies the type of logon page that appears.
  The options are:
  • **401**
    Displays a basic HTTP authentication form.
  • **form-based**
    Displays a logon page.

**See also**

apm, create, delete, edit, list, modify, show, tmsh
message-box

Manages a Message Box agent.

Module

apm policy agent

Syntax

Configure the message-box component within the policy agent module using the syntax shown in the following sections.

Create/Modify

create message-box [name]
modify message-box [name]
options:
    customization-group [string]
edit message-box [ [ [name] | [glob] | [regex] ] ... ]
options:
    all-properties
    non-default-properties

Display

list message-box
list message-box [ [ [name] | [glob] | [regex] ] ... ]
show running-config message-box
show running-config message-box [ [ [name] | [glob] | [regex] ] ... ]
options:
    all-properties
    non-default-properties
    partition
show message-box
show message-box [name]

Delete

delete message-box [name]
Chapter 9

Description

You can use the **message-box** agent to create, display, or delete a Message Box agent.

You cannot use the command line interface to create or modify the messages that display in a message box.

You can also edit customizable messages using the Visual Policy editor.

Examples

Creates the Message Box agent named **MyMessageBoxAgent** that is associated with the customization group named **MyMessageBoxCG**:

```
create message-box MyMessageBoxAgent { customization group "MyMessageBoxCG" }
```

Displays a list of Message Box agents:

```
list message-box
```

Deletes the Message Box agent named **MyMessageBoxAgent**:

```
delete message-box MyMessageBoxAgent
```

Options

You can use these options with the **message-box** component:

- **name**
  
  Specifies the name of a Message Box agent. This option is required.

- **customization-group**
  
  Specifies the name of the customization group that contains the messages you want to apply to an access policy. This option is required.

- **partition**
  
  Displays the partition within which the component resides.

See also

- `apm`
- `create`
- `delete`
- `edit`
- `list`
- `modify`
- `show`
- `tmsh`
oam

Manages an OAM agent.

Module

apm policy agent

Syntax

Configure the oam component within the policy agent module using the syntax shown in the following sections.

Create/Modify

create oam [name]
modify oam [name]
  options:
    max-logon-attempt [integer]
    server [[string] | none]
    show-extended-error [true | false]
    url [[string] | none]
edit oam [ [ [name] | [glob] | [regex] ] ... ]
  options:
    all-properties
    non-default-properties

Display

list oam
list oam [ [ [name] | [glob] | [regex] ] ... ]
show running-config oam
show running-config oam [ [ [name] | [glob] | [regex] ] ... ]
  options:
    all-properties
    non-default-properties
    partition
show oam
show oam [name]

Delete

delete oam [name]
Description

You can use the `oam` component to create and manage an OAM agent.

Examples

Creates an OAM agent named `oam_agent1` that uses authentication server `oam10g` and prompts a user for credentials three times before denying access to `http://www.mydomain.com/protected/`:

```plaintext
create oam oam_agent1 {
    server oam10g
    max-logon-attempt 3
    show-extended-error false
    url "http://www.mydomain.com/protected/"
}
```

Displays a list of OAM agents

```plaintext
list oam all
```

Deletes the OAM agent named `my_tacacsplus_agent`:

```plaintext
delete oam my_oam_agent
```

Options

You can use these options with the `oam` component:

- **name**
  Specifies the name of the component. This option is required.

- **max-logon-attempt**
  Specifies the maximum number of opportunities that users have to re-enter credentials after their first attempt to log in fails. If you set this value to a number from 2 to 5 inclusive, the system allows users the specified number of opportunities to log in after the first attempt to log in fails. If you set the value to 1, the system does not allow a second log in opportunity after a first log in attempt fails. The default value is 3.

- **partition**
  Displays the partition within which the component resides.

- **server**
  Specifies the name of the OAM server used for user authentication. This option is required.

- **url**
  Specifies the URL of the resource that is protected by the OAM server. It is used to authenticate the user using the specified user credentials. This option is required, and you must specify an absolute URL. An absolute URL specifies the exact location of a file or directory on the Internet.
- **show-extended-error**
  Specifies to display a verbose error message on the retry logon page. The default value is `false`.

**See also**

apm, create, delete, edit, list, modify, show, tmsh
resource-assign

Manages a Resource Assign agent.

Module

apm policy agent

Syntax

Configure the resource-assign component within the policy agent module using the syntax shown in the following sections.

Create/Modify

create resource-assign [name]
modify resource-assign [name]

options:
  rules (<string> | none)
  type [acls | general | resources | webtop-and-webtop-links]

edit resource-assign [ [ [name] | [glob] | [regex] ] ... ]

options:
  all-properties
  non-default-properties

Display

list resource-assign
list resource-assign [ [ [name] | [glob] | [regex] ] ... ]
show running-config resource-assign
show running-config resource-assign [ [ [name] | [glob] | [regex] ] ... ]

options:
  all-properties
  non-default-properties
  partition
show resource-assign
show resource-assign [name]

Delete

delete resource-assign [name]
Description

You can use the `resource-assign` component to create and manage an agent that assigns an ACL, a resource group, or both to an access policy. A resource group is a collection of resources, access control lists, and protection criteria, which includes your company intranet servers, applications, and network shares.

An ACL is a set of restrictions associated with a resource or favorite that defines access for users and groups.

Examples

Creates the Resource Assign agent named `MyAssignResourceAgent` and assigns `webtop-link google` when authentication is passed:

```bash
create resource-assign MyAssignResourceAgent my rules {
    { expression "expr { [mcget {session.ad.last.authresult}] == 1 }" 
        webtop-links add { google } 
    }
}
```

Displays a list of Resource Assign agents:

```bash
list resource-assign all
```

Deletes the Resource Assign agent named `MyAssignResourceAgent`:

```bash
delete resource-assign MyAssignResourceAgent
```

Options

You can use these options with the `resource-assign` component:

- **name**
  Specifies the name of the Resource Assign agent. This option is required.

- **partition**
  Displays the partition within which the component resides.

- **rules**
  Adds a rule to or deletes a rule from the Resource Assign agent. You can use the following attributes to define a rule:

  - **acl**
    Specifies an access control list that this rule assigns to users.

  - **connectivity-resource-group**
    Specifies the name of the connectivity resource group to which this rule applies.

  - **expression**
    Specifies the expression that indicates which resource groups this rule assigns to users.
Chapter 9

- **type**
  Specifies the type of Resource Assign agent. The default value is **general**.

See also

apm, create, delete, edit, list, modify, show, tmsh
route-domain-selection

Manages a Route Domain Selection agent.

Module

apm policy agent

Syntax

Configure the route-domain-selection component within the policy agent module using the syntax shown in the following sections.

Create/Modify

create route-domain-selection [name]
modify route-domain-selection [name]
   options:
      route-domain [[integer] | none]
      snat [automap | none]
      snatpool [[string] | none]
edit route-domain-selection [ [ [name] | [glob] | [regex] ] ... ]
   options:
      all-properties
      non-default-properties

Display

list route-domain-selection
list route-domain-selection [ [ [name] | [glob] | [regex] ] ... ]
show running-config route-domain-selection
show running-config route-domain-selection [ [ [name] | [glob] | [regex] ] ... ]
   options:
      all-properties
      non-default-properties
      partition
show route-domain-selection
show route-domain-selection [name]

Delete

delete route-domain-selection [name]
Description

You can use the `route-domain-selection` component to create a Route Domain Selection agent.

Examples

Creates the `my_rds_ag` Route Domain Selection agent:

```
create route-domain-selection my_rds_ag route-domain 0 snat automap
```

Displays a list of Route Domain Selection agents:

```
show route-domain-selection
```

Deletes the Route Domain Selection agent named `my_rd_selection_agent`:

```
delete route-domain-selection my_rd_selection_agent
```

Options

You can use these options with the `route-domain-selection` component:

- **name**
  Specifies the name of a Variable Assignment agent. This option is required.
- **partition**
  Displays the partition within which the component resides.
- **route-domain**
  Specifies the route domain. The default value is 0 (zero).
  - `snatautomap`
  - `none`
    Snat is not used.
- **snatpool**

See also

`apm, create, delete, edit, list, modify, show, tmsh`
tacacsplus

Manages a TACACS+ agent.

Module

apm policy agent

Syntax

Configure the tacacsplus component within the policy agent module using the syntax shown in the following sections.

Create/Modify

create tacacsplus
modify tacacsplus
   options:
      max-logon-attempt [integer]
      server [[string] | none]
edit tacacsplus [ [ [name] | [glob] | [regex] ] ... ]
   options:
      all-properties
      non-default-properties

Display

list tacacsplus
list tacacsplus [ [ [name] | [glob] | [regex] ] ... ]
show running-config tacacsplus
show running-config tacacsplus [ [ [name] | [glob] | [regex] ] ... ]
   options:
      all-properties
      non-default-properties
      partition
show tacacsplus
show tacacsplus [name]

Delete

delete tacacsplus [name]
Description

You can use the \texttt{tacacsplus} component to create and manage a TACACS+ agent.

Examples

Displays a list of TACACS+ agents:
\begin{verbatim}
list tacacsplus all
\end{verbatim}

Deletes the TACACS+ agent named \texttt{my_tacacsplus_agent}:
\begin{verbatim}
delete tacacsplus my_tacacsplus_agent
\end{verbatim}

Options

You can use these options with the \texttt{tacacsplus} component:

\begin{itemize}
  \item \textbf{name}
    Specifies the name of the component. This option is required.
  \item \textbf{max-logon-attempt}
    Specifies the maximum number of opportunities that users have to re-enter credentials after their first attempt to log in fails. If you set this value to a number from 2 to 5 inclusive, the system allows users the specified number of opportunities to log in after the first attempt to log in fails. If you set the value to 1, the system does not allow a second log in opportunity after a first log in attempt fails. The default value is 3.
  \item \textbf{partition}
    Displays the partition within which the component resides.
  \item \textbf{server}
    Specifies the name of the TACACS+ server. This option is required.
\end{itemize}

See also

\texttt{apm, create, delete, edit, list, modify, show, tmsh}
variable-assign

Manages a Variable Assignment agent.

Module

apm policy agent

Syntax

Configure the variable-assign component within the policy agent module using the syntax shown in the following sections.

Create/Modify

create variable-assign [name]
modify variable-assign [name]
  options:
    type [citrix-smart-access | general | intranet-webtop | sso-cred-mapping | virtual-keyboard]
    variables { [varname [name] expression {{[string]}}
edit variable-assign [ [ [name] | [glob] | [regex] ] ... ]
  options:
    all-properties
    non-default-properties

Display

list variable-assign
list variable-assign [ [ [name] | [glob] | [regex] ] ... ]
show running-config variable-assign
show running-config variable-assign [ [ [name] | [glob] | [regex] ] ... ]
  options:
    all-properties
    non-default-properties
    partition
show variable-assign
show variable-assign [name]

Delete

delete variable-assign [name]
Chapter 9

Description

You can use the `variable-assign` component to create and manage an agent that assigns one or more variables to an access policy.

F5 Networks recommends that you use the Visual Policy editor to create complex variable assignments.

Examples

Creates the `username_variable_assign_ag` Variable Assignment agent that automatically assigns the value of the common name field in the client certificate to the username field of the logon page. This is useful when an access policy contains the Variable Assignment agent between the client certification and the AAA Active Directory server query actions:

```plaintext
create variable-assign username_variable_assign_ag {
    variables
        { varname "session.logon.last.username" expression "{{mcget {session.ssl.cert.cn}}}" }
}
```

 Creates a Variable Assignment agent that carries out a configured ACL when a particular branch in the access policy is followed, using the Variable Assignment agent to populate the appropriate variables with the ACL name

```plaintext
create variable-assign acl_variable_assign_ag {
    variables
        { varname "config.connectivity_resource_network_access.MyprofileNR2.acl_name"
            expression "expr {"MY_ACL1"}"
        }
}
```

Displays a list of Variable Assignment agents:

```plaintext
show variable-assign
```

Deletes the Variable Assignment agent named `MyAssignVariableAgent`:

```plaintext
delete variable-assign MyAssignVariableAgent delete
```

Options

You can use these options with the `variable-assign` component:

- **name**
  Specifies the name of a Variable Assignment agent. This setting is required.

- **partition**
  Displays the partition within which the component resides.

- **type**
  Specifies the type of agent. The default value is `general`.  

9 - 100
**variables**

Adds a variable to or deletes a variable from the Variable Assignment agent. You must specify the following attributes for each variable:

- **expression**
  A Tcl expression that the system evaluates, and then assigns the value of the expression to a specific property of the assigned Network Access resource or to a newly created session variable.

- **varname**
  A variable that forms the left-hand side of the expression. You can use the name of an existing variable or a new session variable.

**See also**

apm, create, delete, edit, list, modify, show, tmsh
Introducing the apm profile module

Alphabetical list of components
Introducing the apm profile module

You can use the **tmsh** components that reside within the **apm profile** module to configure BIG-IP® Access Policy Manager®. For more information about the **tmsh** hierarchical structure, see Chapter 2, *Understanding and Using the Traffic Management Shell*.

Alphabetical list of components

The remainder of this chapter lists the **tmsh** components that are available in the **apm profile** module.
access

Configures an access profile.

Module

apm profile

Syntax

Configure the access component within the profile module using the syntax shown in the following sections.

Create/Modify

create access [name]
modify access [name]

options:
accept-languages [add | delete | modify | replace-all-with] {
    [name]
}
access-policy [[string] | none]
access-policy-timeout [integer]
cache-generation [integer]
customization-group [[string] | none]
default-language [[string] | none]
defaults-from [[string] | none]
domain-cookie [[string] | none]
domain-groups [add | delete | modify | replace-all-with] {
    [name]
}
domain-mode [single-domain | multi-domain]
eps-group [[string] | none]
errormap-group [[string] | none]
framework-installation-group [[string] | none]
general-ui-group [[string] | none]
generation-action [increment | noop]
inactivity-timeout [integer]
logout-uri-include [add | delete | modify | replace-all-with] {
    [name]
}
logout-uri-timeout [integer]
max-concurrent-sessions [[integer] | none]
max-concurrent-users [[integer] | none]
max-session-timeout [integer]
persistent-cookie [true | false]
primary-auth-service [string] | none
secure-cookie [true | false]
sso-name [string | none]
edit access [ [ [name] | [glob] | [regex] ] ... ]
  options:
  all-properties
  non-default-properties

Display
list access
list access [ [ [name] | [glob] | [regex] ] ... ]
show running-config access
show running-config access [ [ [name] | [glob] | [regex] ] ... ]
  options:
  all-properties
  non-default-properties
  partition
show access
show access [name]

Delete
    delete access [name]

Description
You can use the access component to configure an access profile. An access profile is a pre-configured group of settings that you can use to configure secure Network Access for an application.

Examples
Creates an access profile named MyAccessProfile that is based on the default access. The profile named access, uses the access policy named my_access-policy, accepts the languages in the my_accepted_languages class, uses English as the default language, and uses these groups to customize the application pages and messages: company_logout, company_header, company_footer, and company_errormap:

```
create access MyAccessProfile {
    defaults-from access
    access-policy "my_access_policy"
    accepted-languages "my_accepted_languages"
```
default-language "en"
customization-group "company_logout"
eps-group 'myepsgroup'
framework-installation-group "company_header" "company_footer"
errormap-group "company_errormap"

Displays a list of access profiles, including parameter values:
list access all all-properties

Deletes the access profile named MyAccessProfile:
delete access MyAccessProfile

Options

You can use these options with the access component:

◆ accept-languages
  Specifies the name of a class that defines the languages supported by the access profile. The default languages are en (English), ja (Japanese), zh-cn (simplified Chinese [PRC]), and zh-tw (traditional Chinese (Taiwan)). This option is required.

◆ access-policy
  Specifies the access policy that you want to enforce using this access profile. An access policy contains various security checks that a client must pass before the BIG-IP® Access Policy Manager® grants access to a protected application. This option is required.

◆ access-policy-timeout
  Specifies, for this access profile, the number of seconds within which a user must complete the steps to gain access to an application. The default value is 300 seconds. This option is designed to quickly release session resources when a user does not complete the access process, for example, when the user closes the browser before completing the access process.

◆ customization-group
  Specifies the customization group that defines the appearance of the logout and error pages. This option is required.

◆ default-language
  Specifies the default language for the BIG-IP Access Policy Manager that you want to implement with this access profile. The default value is en (English). If the client requests a language that is not supported, the BIG-IP Access Policy Manager uses the default value. This option is required.

◆ defaults-from
  Specifies the default access policy from which this profile is created. This option is required.
Domain-Cookie

Domain-cookie

Specifies a domain cookie to use with an application access control connection. If you specify a domain cookie, then the line domain=specified_domain is added to the MRHsession cookie. The default value is none.

Domain-groups

Domain-groups

Specifies a group of multiple domains or multiple hosts in multiple domains to which a single user session has access. For example, you can use this option to configure a single user session to have access to three domains: www.a.com, www.b.com, and www.c.com. When a user logs in to any of these domains, that user can access the other domains without logging in again. This option is required when you set the domain-mode option to multi-domain. For each domain in the domain group, you can specify the following settings:

- cookie-host
  Specifies the host name for which to create the user’s session cookie.

- cookie-domain
  Specifies the domain for which to create the user’s session cookie.

- secure-cookie
  Adds a security attribute to the user’s session cookie.

- persistent-cookie
  Adds a persistence attribute to the user’s session.

- sso-name
  Specifies the SSO method to use when accessing a backend application.

Domain-mode

Domain-mode

Specifies how the SSO configuration is applied.

The options are:

- single-domain
  Applies the SSO configuration to a single domain. This is the default. When you set domain-mode to single-domain, you must also set the sso-name option.

- multi-domain
  Applies the SSO configuration across multiple domains. This option allows users a single APM™ login/session and applies the credentials across multiple Local Traffic Manager™ or Access Policy Manager virtual servers in front of different domains. Note that to apply SSO configurations across multiple domains, all virtual servers must be on one BIG-IP system. When you set domain-mode to multi-domain, you must also configure the domain-group option, and provide a URI for the primary-auth-service option.

Eps-group

Eps-group

This option is required.

Errormap-group

Errormap-group

Specifies the customization settings for the error map that you want to implement with this access profile. This setting is required.
framework-installation-group
Specifies the customization settings for the header and footer that you want to implement with this access profile. This setting is required.

generation-ui-group
Specifies the generation of the user interface group for the new generation access configuration. This option is required.

generation-timeout
Specifies the timeout, in seconds, for the new generation access configuration.

inactivity-timeout
Specifies, for this access profile, the number of seconds that the session on the client can be idle before the server disconnects the VPN tunnel. The default value is 900 seconds.

logout-uri-include
Specifies a list of URIs to include in the access profile for initiating session logout.

logout-uri-timeout
Specifies the timeout used to delay logout for the customized logout URIs defined in the logout uri include list.

max-concurrent-sessions
Specifies, for this access profile, the number of concurrent sessions allowed. The default value is 0 (zero), which represents unlimited sessions. Users assigned an administrative role of Application Editor can view the value of this option. Users assigned any other administrative role can modify this option.

max-concurrent-users
Specifies, for this access profile, the number of concurrent sessions allowed. The default value is 0 (zero), which represents unlimited sessions. This field is read-only for Application Editors. Users assigned any other administrative role can modify this field.

max-session-timeout
Specifies the maximum lifetime of one session. The maximum lifetime is the number of seconds between session creation and session termination.

name
Specifies the name of the access profile. This option is required.

persistent-cookie
Specifies to retain the cookie for a user session, even when the user session is terminated, when set to true. Although this is an insecure method, this setting is useful and required in cases where you have a third-party application, such as Microsoft® SharePoint®, and need to store the cookie in a local database so that any attempt to access backend server applications through Access Policy Manager succeeds. The default value is false.

primary-auth-service
Specifies the address of your primary authentication URI. This setting is required when you set the domain-mode option to multi-domain. For example, when you set this option to https://logon.yourcompany.com,
the user session is stored on this primary domain, and the user can access multiple backend applications from multiple domains and hosts without re-entering credentials.

- **secure-cookie**
  Set this option to true, if you want to add a secure keyword to the session cookie. Set this option to false, if you want to configure an application access control scenario that uses an HTTPS virtual server to authenticate the user, and then sends the user to an existing HTTP virtual server to use applications. The default value is true.

- **sso-name**
  Specifies the SSO configuration that you want BIG-IP Access Policy Manager to use to submit the user’s credentials to the backend application. This allows the user to log in once to the Access Policy Manager and then gain access to backend applications without logging in again.

See also

policy, sso
Chapter 10

connectivity

Configures a connectivity profile.

Module

apm profile

Syntax

Configure the connectivity component within the profile module using the syntax shown in the following sections.

Create/Modify

create connectivity [name]
modify connectivity [name]

options:
   adaptive-compression [enabled | disabled]
   citrix-client-bundle [[name] | default-citrix-client-bundle]
   component-update [yes | prompt | no]
   compress-buffer-size [integer]
   compress-cpu-saver [true | false]
   compress-cpu-saver-high [integer]
   compress-cpu-saver-low [integer]
   compress-gzip-level [integer]
   compress-gzip-memlevel [integer]
   compress-gzip-window-size [integer]
   compress-ingress [true | false]
   compress-preferred-method [[string] | none]
   compression [enabled | disabled]
   compression-codecs [[string] | none]
   customization-group [[string] | none]
   defaults from [[name] | none]
   deflate-compression-level [integer]
   enforce-session-settings [true | false]
   location-dns [[string] | none]
   reuse-winlogon-creds [true | false]
   save-password [true | false]
   save-password-method [disk | memory]
   save-password-timeout [integer]
   save-servers-on-exit [true | false]
   servers [add | delete | modify | replace-all-with] { [name]
You can use the **connectivity** component to configure a connectivity profile. By using the connectivity profile, you can configure L2 and L4 tunnels, compression, Windows and mobile client settings, and client component downloads from F5 Networks and Citrix.

**Examples**

Creates a connectivity profile named `myconnectivityprofile` that inherits its settings from the system default connectivity profile:

```bash
create connectivity myconnectivityprofile {}
```
Options

You can use these options with the **connectivity** component:

- **adaptive-compression**
  Enables or disables adaptive compression. Use this option to configure compression settings for application tunnels and to optimize applications and RDP traffic. The default value is **enabled**.

- **citrix-client-bundle**
  Specifies the Citrix client bundle used by this connectivity profile. The default value is **default-citrix-client-bundle**.

- **component-update**
  Specifies how the Secure Access Client handles automatic updates. The options are:
  - **yes**
    Automatically installs a client update when one is available.
  - **prompt**
    Prompts the user about installing a client update.
  - **no**
    Disables the client from receiving automatic updates.

- **compress-buffer-size**
  Specifies the size of compressed data for Network Access tunnels. The default value is **4096**.

- **compress-cpu-saver**
  Specifies whether the system monitors the percentage of CPU usage and adjusts compression rates automatically when CPU usage reaches either the CPU saver high threshold or the CPU saver low threshold. The default value is **true**.

- **compress-cpu-saver-high**
  Specifies the percentage of CPU usage at which the system starts automatically decreasing the amount of content being compressed, as well as the amount of compression which the system is applying. The default value is **90** percent.

- **compress-cpu-saver-low**
  Specifies the percentage of CPU usage at which the system resumes content compression at the user-defined rates. The default value is **75** percent.

- **compress-gzip-level**
  Specifies the degree to which the system compresses the content. Higher compression levels slow down the compression process. The default value is **6**, which provides a higher amount of compression at the expense of more CPU processing time. **1** is the lowest level and **9** is the highest level. **0** (zero) disables compression.

- **compress-gzip-memlevel**
  Specifies the number of kilobytes of memory that the system uses for internal compression buffers when compressing data. You can select a value between 1 and 256. The default value is **8192**.
◆ **compress-gzip-window-size**
   Specifies the number of kilobytes in the window size that the system uses when compressing data. You can select a value between 1 and 128. The default value is 16384.

◆ **compress-ingress**
   Specifies whether incoming data is compressed. The default value is false.

◆ **compress-preferred-method**
   Specifies the preferred method of data compression. The default value is zlib.

◆ **compression**
   Enables or disables compression between the client and the server. The default value is enabled.

◆ **compression-codecs**
   Specifies the available compression codecs for server-to-client connections. The server compares the available compression types you configure with the available compression types on the client, and then chooses the most effective mutual compression setting. Compression for the client is configured separately. The default includes all three available codecs.

   The options are:
   - lzo
     Offers a balance between CPU resources and compression ratio, compressing more than deflate, but with less CPU resources than bzip2.
   - deflate
     Uses the least CPU resources, but compresses the least effectively.
   - bzip2
     Uses the most CPU resources, but compresses the most effectively.

◆ **customization-group**
   Specifies which customization groups are applied. This option is required.

◆ **defaults-from**
   Specifies the profile from which this profile inherits properties that are not specified explicitly. The default value is connectivity.

◆ **deflate-compression-level**
   Specifies the level of compression performed by the deflate codec. The default value is 1.

◆ **enforce-session-settings**
   Specifies whether Secure Access Client always honors the session settings configured by the administrator on the server, or can use settings selected by the user. The default value is false.

   The options are:
   - false
     Ensures that the Secure Access Client always uses the session settings configured on the server.
true
Ensures that the Secure Access Client uses settings chosen by the user.

location-dns
Specifies a list of DNS suffixes used by the Network Location Awareness feature of the Secure Access Client. This list represents the internal network where local resources are available without the need of a Network Access connection. The default value is none.

name
Specifies the profile that you want to use as the parent profile. The new profile inherits all settings and values from the parent profile.

reuse-winlogon-creds
Specifies whether Secure Access Client can reuse logon credentials entered by a user for a subsequent log in. The default value is false.

save-password
Specifies whether Secure Access Client allows user password caching. The default value is true.

save-password-method
Specifies whether Secure Access Client saves encrypted passwords on disk or caches passwords in memory only. The default value is disk.

save-password-timeout
Specifies the number of minutes that a cached password remains valid (applies only to in-memory password caching). The default value is 240.

save-servers-on-exit
Specifies whether Secure Access Client maintains a list of Access Policy Manager systems that the client accessed. The default value is true.

servers
Specifies a list of server and alias pairs in the Secure Access Client's server list. Delimit server and alias entries using double colons ("::"). For example, "server1::alias2".

tunnel-name
Specifies the name of the tunnel through which data passes. The default value is none.

win-mobile-server
Specifies a server URL to which Secure Access Client for Windows Mobile can connect. The default value is none.

win-mobile-work-url-exceptions
Specifies IP addresses and domain names that can be accessed through Secure Access Client, for example 192.168.*, *.company.com, server.company.com. The default value is none.

See also
profile, virtual
remote-desktop

Displays information about a default profile that supports a Citrix remote desktop resource.

Module

apm profile

Syntax

Displays the properties of the remote-desktop component within the profile module.

Display

list remote-desktop
list remote-desktop [ [name] | [glob] | [regex] ] ...
show running-config remote-desktop
show running-config remote-desktop [ [glob] | [regex] ] ...

options:
  all-properties
  non-default-properties
  one-line

Description

You can use the remote-desktop component to display the properties of the default remote desktop profile.

Examples

Displays all of the properties of the default remote desktop profile:

list remotedesktop all-properties

See also

profile, ltm virtual
Chapter 10

**rewrite**

Configures a rewrite profile for client caching.

**Module**

apm profile

**Syntax**

Configure the rewrite component within the profile module using the syntax shown in the following sections.

**Create/Modify**

create rewrite [name]

modify rewrite [name]

  options:
  bypass-list [add | delete | none | replace-all-with] {
    [uri list]
  }
  client-caching-type [cache-all | cache-css-js | cache-img-css-js | no-cache]
  defaults-from [[string] | none]
  rewrite-list [add | delete | none | replace-all-with] {
    [uri list]
  }
  split-tunneling [true | false]

edit rewrite [ [ [name] | [glob] | [regex] ] ... ]

  options:
  all-properties
  non-default-properties

**Display**

list rewrite

list rewrite [ [ [name] | [glob] | [regex] ] ... ]

show running-config rewrite

show running-config rewrite [ [ [name] | [glob] | [regex] ] ... ]

  options:
  all-properties
  app-service
  non-default-properties
  partition

show running-config rewrite [ [ [name] | [glob] | [regex] ] ... ]
Delete

```
dele te rewrite [name]
```

Description

You can use the `rewrite` component to configure a Rewrite profile for client caching and the rewrite/bypass list (split tunneling) for web application access.

Examples

Creates a rewrite profile name `new_rewrite_profile` that allows split tunneling:

```
create rewrite new_rewrite_profile split-tunneling true rewrite-list add {
  *://www.myportal.com/* http://abc*.com/* }
bypass-list add { *://external_web.com/* }
```

Modifies the `new_rewrite_profile` to configure the client to cache all files:

```
modify rewrite new_rewrite_profile client-caching-type cache-all
```

Displays the properties of `new_rewrite_profile`:

```
list rewrite new_rewrite_profile all-properties
```

Options

You can use these options with the `rewrite` component:

- `bypass-list`
  Specifies a list of URIs that are bypassed inside a web page when the page is accessed using portal access. The default value is `none`.

- `client-caching-type`
  Specifies one of four options for client caching. When the Client Cache setting for a web application resource is set to `default`, the system uses the setting configured in the Rewrite profile. If the Client Cache option is configured for any other setting, the web application resource item caching configuration overwrites the setting in the Rewrite profile. The default value is `cache-css-js`.

  The options are:
  - `cache-all`
    Do not modify cache headers on backend servers.
  - `cache-css-js`
    Cache only the CSS file and Java Script.
  - `cache-img-css-js`
    Cache only images, the CSS file and Java Script.
  - `no-cache`
    Eliminate caching.
Chapter 10

◆ defaults-from
   Specifies the profile from which the Rewrite profile inherits properties. Explicitly specified properties override inherited properties.

◆ name
   Specifies a unique name for the component. This option is required.

◆ rewrite-list
   Specifies a list of URIs that are rewritten inside a web page when the page is accessed using portal access. The default value is none.

◆ split-tunneling
   Specifies whether the profile provides for split tunneling. The default value is false.

See also

profile
apm resource Module Components

- Introducing the apm resource module
- Alphabetical list of components
Introducing the apm resource module

You can use the tmsh components that reside within the apm resource module to configure BIG-IP® Access Policy Manager®. For more information about the tmsh hierarchical structure, see Chapter 2, *Understanding and Using the Traffic Management Shell*.

Alphabetical list of components

The remainder of this chapter lists the tmsh components that are available in the apm resource module.
app-tunnel

Configures an application tunnel.

Module

apm policy

Syntax

Configure the app-tunnel component within the resource module using the syntax shown in the following sections.

Create/Modify

create app-tunnel [name]
modify app-tunnel [name]

options:
  acl-order [integer]
  app-service [[string] | none]
  application-launch-warning [true | false]
  apps [add | delete | modify | replace-all-with] {
    [name]
  }
  customization-group [add | delete | modify | replace-all-with] {
    [name]
  }
  description [[string] | none]
  type [app-tunnel | last | network-access | remote-desktop | web-application]

edit app-tunnel [ [ [name] | [glob] | [regex] ] ... ]

options:
  all-properties
  non-default-properties

Display

list app-tunnel
list app-tunnel [ [ [name] | [glob] | [regex] ] ... ]
show running-config app-tunnel
show running-config app-tunnel [ [ [name] | [glob] | [regex] ] ... ]

options:
  all-properties
  non-default-properties
  one-line
show app-tunnel
show app-tunnel [name]

Delete

delete app-tunnel [name]

Description

You can use the app-tunnel component to configure an application tunnel to provide secure access to a network, remote desktop, or specific applications.

Examples

Creates an application tunnel named myapptunnel that uses the policies in the customization group myapptunnelcg:
create app-tunnel myapptunnel customization-group myapptunnelcg

Deletes the application tunnel named myapptunnel:
delete app-tunnel myapptunnel

Options

You can use these options with the app-tunnel component:

◆ acl-order
   Specifies the location of this app tunnel in the ACL hierarchy in Access Policy Manager ACL lists. The default value is 0 (zero).

◆ app-service
   The default value is none.

◆ application-launch-warning
   Specifies whether to display a warning before launching an application.
   The options are:
   ● true
      The system displays security warnings before launching an application, regardless of whether the site is considered a Trusted site. This is the default value.
   ● false
      The system displays security warnings before launching an application, only if the site is not in the Trusted Sites list.

◆ apps
   Specifies the applications that a user can access using this application tunnel. The default value is none.
◆ customization-group
   Specifies whether customizations are applied to the application tunnel. You can add, modify, delete, or replace all customization groups. This option is required.

◆ description
   Specifies a description for the application tunnel. The default value is none.

◆ name
   Specifies a name for the component.

◆ partition
   Displays the partition within which the app-tunnel component resides. The default value is common.

◆ type
   Specifies the type of application tunnel.
   The options are:
   • app-tunnel
     This is the default.
   • network-access
     Provides access to a network.
   • remote-desktop
     Provides access to a remote desktop.

◆ web-application
   Provides access to a web application.

See also

apm, create, delete, edit, list, modify, show, tmsh
client-rate-class

Configures a client rate class resource.

Module

apm policy

Syntax

Configure the client-rate-class component within the resource module using the syntax shown in the following sections.

Create/Modify

create client-rate-class [name]
modify client-rate-class [name]
  options:
    app-service [[string] | none]
    burst [integer]
    ceiling [integer]
    description [[string] | none]
    dscp [integer]
    mode [borrow | discard | shape]
    rate [integer]
    type [best-effort | controlled-load | guaranteed]
edit client-rate-class [ [ [name] | [glob] | [regex] ] ... ]
  options:
    all-properties
    non-default-properties

Display

list client-rate-class
list client-rate-class [ [ [name] | [glob] | [regex] ] ... ]
show running-config client-rate-class
show running-config client-rate-class [ [ [name] | [glob] | [regex] ] ... ]
  options:
    all-properties
    non-default-properties
show client-rate-class
show client-rate-class [name]
Delete

```
delete client-rate-class [name]
```

Description

You can use the `client-rate-class` component to configure a client rate class resource, which is used in traffic control.

Examples

Creates a client rate class resource named `sf1` used in traffic control, sets the `dscp` to 40 and the rate to 60000, sets the ceiling to 80000, and sets the mode to `shape`:

```
create client-rate-class sf1{
    dscp 40
    rate 60000
    ceiling 80000
    mode shape
}
```

Displays a list of all client rate class on the system:

```
list client-rate-class all
```

Deletes the client rate class named `sf1` from the system:

```
delete client-rate-class sf1
```

Options

You can use these options with the `client-rate-class` component:

- **burst**
  Specifies in bytes the maximum amount of data that can reach the ceiling rate at one time. The default value is 0 (zero).

- **ceiling**
  Specifies how far, beyond the value specified for the rate option, that traffic can flow when bursting. This number sets an absolute limit. No traffic can exceed this rate. The rate class might limit traffic throughput to the value of the rate option when there is high contention among siblings of a parent-child class hierarchy. The default value is the value of the rate option. The minimum value is 296 bits per second (bps).

- **description**
  Specifies a description for the client rate class. The default value is `none`.

- **dscp**
  Specifies six bits of DS field that are used as a codepoint to select the Per Hop Behavior (PHB) for a packet in each network node. The default value is `-1`. 
◆ **name**
   Specifies a unique name to identify the client rate class.

◆ **mode**
   Specifies the mode to use for this client rate class.
   The options are:
   - **borrow**
     Allows traffic on the client rate class to borrow resources from other flows that are temporarily idle. Traffic that borrows resources is marked as nonconforming and receives a lower priority. This is the default.
   - **discard**
     Discards packets that do not conform to the specified traffic control descriptor.
   - **shape**
     Delays packets submitted for transmission until the packets conform to the specified flow parameters.

◆ **partition**
   Displays the partition within which this component resides. The default value is **common**.

◆ **rate**
   Specifies the guaranteed throughput rate of the traffic handled by this rate class. You can configure the rate in bits per second (bps), kilobits per second (Kbps), megabits per second (Mbps), or gigabits per second (Gbps).

◆ **type**
   Specifies the service type in use for the client rate class.
   The options are:
   - **best-effort**
     Microsoft® Windows® traffic control creates a flow for this client traffic class, and traffic on the flow is handled with the same priority as other Best Effort traffic. This is the default.
   - **controlled-load**
     Traffic control transmits a very high percentage of packets to the intended receivers. Packet loss for this type closely approximates the basic packet error rate of the transmission medium. Transmission delay for a very high percentage of the delivered packets does not greatly exceed the minimum transit delay experienced by any successfully delivered packet.
   - **guaranteed**
     Guarantees that datagrams arrive within a specified delivery time and will not be discarded due to queue overflows, provided that the flow of traffic stays within specified traffic parameters. This type is intended for applications that require guaranteed packet delivery.
See also

apm, create, delete, edit, list, modify, show, tmsh
client-traffic-classifier

Configures client traffic classifier entries.

Module

apm resource

Syntax

Configure the client-traffic-classifier component within the resource module using the syntax shown in the following sections.

Create/Modify

create client-traffic-classifier [name]
modify client-traffic-classifier [name]

options:
  entries [add | delete | modify | replace-all-with] {
    [name] {
      client-rate-class [[string] | none]
dst-ip [[ipv4 address] | none]
dst-mask [[integer] | none]
dst-port [[integer] | none]
protocol [[integer] | none]
src-ip [[ipv4 address ] | none]
src-mask [[integer] | none]
src-port [[integer] | none]
    }
  }
edit client-traffic-classifier [ [ [name] | [glob] | [regex] ] ... ]

options:
  all-properties
  non-default-properties

Display

list client-traffic-classifier
list client-traffic-classifier [ [ [name] | [glob] | [regex] ] ... ]
show running-config client-traffic-classifier
show running-config client-traffic-classifier [ [ [name] | [glob] | [regex] ] ... ]

options:
  all-properties
  app-service
non-default-properties
one-line
partition
show client-traffic-classifier
show client-traffic-classifier [name]

Delete
delete client-traffic-classifier [name]

Description
You can use the client-traffic-classifier component to configure a client traffic classifier, which is used by traffic control agent.

Examples
Creates a client traffic classifier named tf1, sets the entry to entry1, the protocol to 6, the DST IP to 192.168.0.0, the DST mask to 255.255.0.0, the DST port to 0 (zero), and the client rate class to sf1:
create client-traffic-classifier tf1
  entries entry1 {
    protocol "6"
    dst-ip "192.168.0.0"
    dst-mask "255.255.0.0"
    dst-port "0"
    client-rate-class "sf1"
  }
  entry2{
    protocol "6"
    src-ip "10.10.0.0"
    src-mask "255.255.255.0"
    client-rate-class "sf2"
  }
}

Displays a list of all client traffic classifiers on the system:
list client-traffic-classifier all

Modifies the client traffic classifier named tf1:
modify client-traffic-classifier tf1 entries entry1 protocol 17

Deletes the client traffic classifier named tf1 from the system:
delete client-traffic-classifier tf1
Options

You can use these options with the `client-traffic-classifier` component:

- **dst-ip**
  Specifies the IP address of the receiver of the packet.

- **dst-mask**
  Specifies the subnet mask for the destination address.

- **dst-port**
  Specifies the 16-bit number to identify the sending port for either UDP or TCP network application.

- **name**
  Specifies the name of the component.

- **partition**
  Displays the partition within which the component resides. The default value is `Common`.

- **protocol**
  Specifies which traffic protocol to use in the filtering rule.

- **src-ip**
  Specifies the address from which the packet is being sent.

- **src-mask**
  Specifies the subnet mask for the source address.

- **src-port**
  Specifies a 16-bit number to identify the sending port for either UDP or TCP network application.

See also

`apm`, `create`, `delete`, `edit`, `list`, `modify`, `show`, `tmsh`
ipv6-leasepool

Configures a lease pool.

Module

apm resource

Syntax

Configure the ipv6-leasepool component within the resource module using the syntax shown in the following sections.

Create/Modify

create ipv6-leasepool [name]
modify ipv6-leasepool [name]

options

description [[string] | none]
members [add | delete | modify | replace-all-with] {
    [[first ip address in range] - [last ip address in range]]
}

Display

list ipv6-leasepool
list ipv6-leasepool [ [ [name] | [glob] | [regex] ] ... ]
show running-config ipv6-leasepool
show running-config ipv6-leasepool [ [ [name] | [glob] | [regex] ] ... ]
options:
    all-properties
    non-default-properties
    one-line
    partition

show ipv6-leasepool
show ipv6-leasepool [name]

Delete

delete ipv6-leasepool [name]
Description

Configures an IPv6 lease pool to create a collection of IPv6 addresses grouped as a single object. You can use a lease pool to associate that collection of IP addresses with a network access resource.

Examples

Creates an IPv6 lease pool named **myipv6-leasepool** that contains the IPv6 addresses in the range **fd1f::1 - fd1f::64**:

```text
create ipv6-leasepool myipv6-leasepool {fd1f::1-fd1f::64}>
```

◆ Note

*No spaces are allowed between the first IPv6 address, hyphen, and second IPv6 address.*

Options

You can use these options with the **ipv6-leasepool** component:

◆ **description**
  Specifies a unique description of the lease pool.

◆ **name**
  Specifies a unique name for the lease pool.

◆ **members**
  Specifies a range of IPv6 addresses separated by a hyphen.

◆ **partition**
  Displays the partition within which the component resides. The default value is **Common**.

See also

**apm, create, delete, edit, list, modify, show, tmsh**
leasepool

Configures a lease pool.

Module

apm resource

Syntax

Configure the leasepool component within the resource module using the syntax shown in the following sections.

Create/Modify

create leasepool [name]
modify leasepool [name]
  options
    description [string] | none
    members [add | delete | modify | replace-all-with] {
      [[first ip address in range] - [last ip address in range]]
    }

Display

list leasepool
list leasepool [ [name] | [glob] | [regex] ] ...
show running-config leasepool
  show running-config leasepool [ [name] | [glob] | [regex] ] ...
    options:
      all-properties
      non-default-properties
      one-line
      partition
show leasepool
show leasepool [name]

Delete

delete leasepool [name]
Description

Configures a lease pool to create a collection of IPv4 addresses grouped as a single object. You can use a lease pool to associate that collection of IPv4 addresses with a network access resource.

Examples

Creates a leasepool named `myleasepool` that contains the IPv4 addresses in the range `10.10.10.1-10.10.10`:

```
create leasepool myleasepool {10.10.10.1-10.10.10}
```

◆ Note

`No spaces are allowed between the first IPv4 address, hyphen, and second IPv4 address.`

Options

You can use these options with the `leasepool` component:

◆ **description**
  Specifies a unique description of the lease pool.

◆ **name**
  Specifies a unique name for the lease pool.

◆ **members**
  Specifies a range of IP addresses separated by a hyphen.

◆ **partition**
  Displays the partition within which the component resides. The default value is `Common`.

See also

`apm, create, delete, edit, list, modify, show, tmsh`
network-access

Configures general settings for a network access connection.

Module

apm resource

Syntax

Configure the network-access component within the resource module using the syntax shown in the following sections.

Create/Modify

create network-access [name]
modify network-access [name]

options:
  address-space-dhcp-requests-excluded [true | false]
  address-space-exclude-subnet [[string] | none]
  ipv6-address-space-exclude-subnet [[string] | none]
  address-space-include-dns-name [[string] | none]
  address-space-include-subnet [[string] | none]
  ipv6-address-space-include-subnet [[string] | none]
  address-space-local-subnets-excluded [true | false]
  address-space-protect [true | false]
  application-launch [[string] | none]
  application-launch-warning [true | false]
  client-interface-speed [[integer] | none]
  client-ipv4-filter-engine [true | false]
  client-power-management [ignore | prevent | terminate]
  client-proxy [true | false]
  client-proxy-address [ip addr]
  client-proxy-exclusion-list [[string] | none]
  client-proxy-local-bypass [true | false]
  client-proxy-port [[integer] | none]
  client-proxy-script [[string] | none]
  client-proxy-use-http-pac [true | false]
  client-traffic-classifier [[string] | none]
  compression [gzip | none]
  customization-group [[string] | none]
  description [[string] | none]
  dns-primary [ip addr]
  ipv6-dns-primary [ip addr]
dns-secondary [ip addr]
ipv6-dns-secondary [ip addr]
dns-suffix [(string) | none]
drive-mapping [(string) | none]
dtls [true | false]
dtls-port [(integer) | none]
execute-logoff-scripts [true | false]
idle-timeout-threshold [(integer) | none]
idle-timeout-window [(integer) | none]
leasepool-name [(string) | none]
ipv6-leasepool-name [(string) | none]
microsoft-network-client [true | false]
microsoft-network-server [true | false]
network-tunnel [enabled | disabled]
opimized-app [add | delete | modify | none | replace-all-with ]
provide-client-cert [true | false]
proxy-arp [true | false]
split-tunneling [true | false]
static-host [(string) | none]
supported-ip-version [ipv4 | ipv4-ipv6]
sync-with-active-directory [true | false]
type [app-tunnel | last | network-access | remote-desktop | web-application]
wins-primary [ip addr]
wins-secondary [ip addr]
edit network-access [ [ [name] | [glob] | [regex] ] ... ]

options:
all-properties
non-default-properties

Display

list network-access
list network-access [ [ [name] | [glob] | [regex] ] ... ]
show running-config network-access
show running-config network-access [ [ [name] | [glob] | [regex] ] ... ]

options:
all-properties
non-default-properties
one-line
partition
show network-access
show network-access [name]
Delete

```
delete network-access [name]
```

Description

You can use the `network-access` component to configure the general settings for a network access connection.

Examples

Creates a network access connection configuration object named `mynetwork-access` that uses the policies in the customization group named `mynetaccess`:

```
create network-access mynetwork-access customization-group mynetaccess
```

Deletes the network access connection configuration object named `mynetwork-access`:

```
delete network-access mynetwork-access
```

Options

You can use these options with the `network-access` component:

- **address-space-dhcp-requests-excluded**
  Specifies whether requests from IP addresses using DHCP are excluded from accessing the network. The default value is `true`.

- **address-space-exclude-subnet**
  Specifies the IPv4 address spaces whose traffic you want to exclude from access to a subnet on the network. The default value is `none`.

- **ipv6-address-space-exclude-subnet**
  Specifies the IPv6 address spaces whose traffic you want to exclude from access to a subnet on the network. The default value is `none`.

- **address-space-include-dns-name**
  Specifies a list of domain names describing the target LAN DNS addresses for split tunneling only. You can add multiple address spaces to the list. For each address space, type the domain name, in the form `site.siterequest.com` or `*.siterequest.com`. The default value is `none`.

- **address-space-include-subnet**
  Specifies a list of IPv4 addresses or address/mask pairs describing the target LAN. When using split tunneling, only the traffic to these addresses and network segments goes through the tunnel configured for Network Access. You can add multiple address spaces to the list. For each address space, type the IPv4 address and network mask. The default value is `none`. 
◆ **address-space-local-subnets-excluded**
   Specifies whether to exclude local access to any host or subnet in routes that you have specified in the client routing table. The default value is **false**. When you set this option to **true**, the system does not support integrated IP filtering.

◆ **address-space-protect**
   Specifies whether the IP address spaces whose traffic is forced through the tunnel are protected. The default value is **false**.

◆ **app-service**
   The default value is **none**.

◆ **application-launch**
   Specifies the applications to launch when the client accesses the network. The default value is **none**.

◆ **application-launch-warning**
   Specifies whether the user is warned that an application is being launched. The default value is **true**.

◆ **client-interface-speed**
   Specifies the baud rate of the client interface with the network. The default value is **100000000**.

◆ **client-ip-filter-engine**
   Specifies whether the client IP address is filtered. The default value is **false**.

◆ **client-power-management**
   Specifies how to interact with Windows system power management features.
   - **prevent**
     Prevents Windows from entering standby/hibernate during connection.
   - **terminate**
     Terminate network access connection if Windows is entering standby/hibernate.
   - **ignore**
     Do nothing. Ignore power management events. This is the default value.

◆ **client-proxy**
   Specifies whether this resource handles a client proxy. The default value is **false**.

◆ **client-proxy-address**
   Specifies the IP address of the proxy client. The default value is **any6**.

◆ **client-proxy-exclusion-list**
   Specifies the web addresses that do not need to be accessed through your proxy server. You can use wild cards to match domain and host names or addresses, for example, **www.*.com, 128.*, 240.8. 8., mygroup.*, and *.**. The default value is **none**.

◆ **client-proxy-local-bypass**
   Specifies whether you want to allow local (intranet) addresses to bypass the proxy server. The default value is **false**.
- **client-proxy-port**
  Specifies the port number of the proxy server you want Network Access clients to use to connect to the Internet. The default value is 0 (zero).

- **client-proxy-script**
  Specifies the URL for a proxy auto-configuration script, if one is used with this connection. The default value is none.

- **client-proxy-use-http-pac**
  Specifies whether the browser uses http:// to locate the proxy the autoconfig file, instead of file://. Set this to true for applications, like Citrix MetaFrame, that cannot use the client proxy autoconfig script when the browser attempts to use the prefix file:// to locate the script. The default value is false.

- **client-traffic-classifier**
  Specifies a client traffic classifier to use with this network access connection. The default value is none.

- **compression**
  Specifies whether you want to compress all traffic between the Network Access client and the controller. The default value is none.

- **customization-group**
  Specifies the customization group that defines the policies that apply to network access. This option is required.

- **description**
  Specifies a unique description of the network access configuration object. The default value is none.

- **dns-primary**
  For split tunneling, specifies the IPv4 address of the primary name server that is conveyed to the remote access point for IPv4 traffic. The default value is any6.

- **ipv6-dns-primary**
  For split tunneling, specifies the IPv6 address of the primary name server that is conveyed to the remote access point for IPv6 traffic. The default value is any6.

- **dns-secondary**
  For split tunneling, specifies the IPv4 address of the secondary name server that is conveyed to the remote access point for IPv4 traffic. The default value is any6.

- **ipv6-dns-secondary**
  For split tunneling, specifies the IPv6 address of the secondary name server that is conveyed to the remote access point for IPv6 traffic. The default value is any6.

- **dns-suffix**
  Type in a DNS suffix to send to the client. If this field is left blank, the controller sends its own DNS suffix. You can specify multiple default domain suffixes separated with commas. The default value is none.

- **drive-mapping**
  For split tunneling, specifies the drive to which this resource provides a network access connection. The default value is none.
◆ **dtls**
   Specifies whether the network access connection uses Datagram Transport Level Security (DTLS). DTLS uses UDP instead of TCP, to provide better throughput for high demand applications like VoIP or streaming video, especially with lossy connections. The default value is **false**.

◆ **dtls-port**
   Specifies the port number that the network access resource uses for secure UDP traffic with DTLS. The default value is **4433**.

◆ **execute-logoff-scripts**
   Specifies whether the system executes logoff scripts (configured on the Active Directory domain) when the connection is terminated. The default value is **false**.

◆ **idle-timeout-threshold**
   Defines the average byte rate that either ingress or egress tunnel traffic must exceed for the tunnel to update a session. If the average byte rate falls below the specified threshold, the system applies the inactivity timeout, which is defined in the session's Access Profile. The default value is **0** (zero).

◆ **idle-timeout-window**
   Defines the value that the system uses to calculate the EMA (Exponential Moving Average) byte rate of ingress and egress tunnel traffic. The default value is **0** (zero).

◆ **leasepool-name**
   Specifies the IPv4 lease pools that the user can access with this network access connection. The default value is **none**.

◆ **ipv6-address-space-include-subnet**
   Specifies a list of IPv6 addresses or address/mask pairs describing the target LAN. When using split tunneling, only the traffic to these addresses and network segments goes through the tunnel configured for Network Access. You can add multiple address spaces to the list. For each address space, type the IPv6 address and network mask. The default value is **none**.

◆ **ipv6-leasepool-name**
   Specifies the IPv6 lease pools that the user can access with this network access connection. The default value is **none**.

◆ **microsoft-network-client**
   Specifies whether the client PC can access remote resources over a VPN connection. The default value is **true**.

◆ **microsoft-network-server**
   Specifies whether the server can access remote resources over a VPN connection. The default value is **false**.

◆ **network-tunnel**
   Enables or disables the network tunnel. The default value is **enabled**.
◆ **optimized-app**
   Specifies the optimized applications that you want to users to access using this network access connection resource. You can add, delete, modify, or replace the current optimized applications. The default value is *none*.

◆ **partition**
   Displays the partition within which this network access connection component resides. The default value is *Common*.

◆ **provide-client-cert**
   Specifies whether client certificates are required to establish an SSL connection. You can set this option to *false* if the client certificates are only requested in an SSL connection. In this case, the client is configured to not send client certificates. The default value is *true*.

◆ **proxy-arp**
   Select *enable* to enable Proxy ARP for this network access resource. When you implement Proxy ARP for a network access resource, remote VPN tunnel clients can use IP addresses from the LAN IP subnet without additional network infrastructure changes. Ranges of IP addresses from the LAN subnet can be configured in the lease pools and assigned to tunnel clients. When a host on the LAN sends traffic to a tunnel client, an ARP query is sent to request the client address. Access Policy Manager then responds with its own MAC address. Traffic is then sent to network access and forwarded to the client over the network access tunnel. No configuration changes are required on devices other than the Access Policy Manager.

   See your Network Access documentation for more information about Proxy ARP configuration. The default value is *false*.

◆ **split-tunneling**
   Specifies whether only traffic targeted to a specified address space is sent over the network access tunnel. With split tunneling, all other traffic bypasses the tunnel. The default value is *false*. When you set this option to *true*, all traffic passing over the network access connection uses this setting.

◆ **static-host**
   Specifies the static hosts to which this resource provides a network access connection. The default value is *none*.

◆ **supported-ip-version**
   Specifies the supported IP protocol version. The default value is *ipv4*.

◆ **sync-with-active-directory**
   Specifies whether you want the network access connection to emulate the Windows logon process for a client on an Active Directory domain. The default value is *false*.

   When this option is set to *true*, network policies are synchronized when the connection is established, or at logoff. The following items are synchronized:
   - Logon scripts are started as specified in the user profile.
   - Drives are mapped as specified in the user profile.
Group policies are synchronized as specified in the user profile. Group Policy logon scripts are started when the connection is established, and Group Policy logoff scripts are run when the network access connection is stopped.

- **type**
  Specifies the type of network access connection this component provides. The default value is `network-access`.

- **wins-primary**
  Specifies the primary IP address to which this resource provides a network access connection. The default value is `any6`.

- **wins-secondary**
  Specifies the secondary IP address to which this resource provides a network access connection. The default value is `any6`.

**See also**

apm, create, delete, edit, list, modify, show, tmsh
portal-access

Configure the portal-access component within the resource module using the syntax shown in the following sections.

Module

apm resource

Syntax

Configure the portal-access component within the resource module using the syntax shown in the following sections.

Create/Modify

create portal-access [name]
modify portal-access [name]

options:
   acl-order [integer]
   application-uri [string] | none
   css-patching [true | false]
   customization-group [string] | none
   description [string] | none
   flash-patching [true | false]
   host-replace-string [string] | none
   host-search-strings [string] | none
   html-patching [true | false]
   items [add | delete | modify | replace-all-with] {
      [string]
   }
   javascript-patching [true | false]
   patching-type [full-patch | min-patch]
   path-match-case [true | false]
   proxy-host [string] | none
   proxy-port [string] | none
   publish-on-webtop [true | false]
   scheme-patching [true | false]

edit portal-access [ all-properties | non-default-properties ]

options:
   all-properties
   non-default-properties
Display

list portal-access
list portal-access [ [ [name] | [glob] | [regex] ] ... ]
show running-config portal-access
show running-config portal-access [ [ [name] | [glob] | [regex] ] ... ]
  options:
    all-properties
    non-default-properties
    one-line
    partition
show portal-access
show portal-access [name]

Delete

delete portal-access [name]

Description

You can use the portal-access component to specify a portal access resource.

Examples

Creates a portal access resource named myportalaccess:

create portal-access myportalaccess acl-order 14 patching-type full-patch items add {
  item1 { host www.mywebsite.com paths /* }}

Deletes the portal access resource named myportalaccess:

delete portal-access myportalaccess

Options

You can use these options with the portal-access component:

- **acl-order**
  Specifies the order of this portal access in Access Policy Manager ACL lists. This option is required.

- **application-uri**

- **css-patching**
  Specifies whether the response content type CSS is patched. The default value is true.

- **customization-group**
  The customization group is created automatically if not specified.
◆ description
   Specifies a description of the resource. The default value is none.

◆ flash-patching
   Specifies whether the system patches Flash content. The default value is true.

◆ host-replace-string
   Specifies the replacement host string, when you specify minimal for the patching-type option.

◆ host-search-strings
   Specifies the host string to replace, when you specify minimal for the patching-type option.

◆ html-patching
   Specifies whether the system patches HTML content. The default value is true.

◆ items
   Configures the host name or IP address, the network mask (if the resource is a network), the port, and any paths specified for a portal access resource. The default value is none.

◆ javascript-patching
   Specifies whether the system patches JavaScript™ content. The default value is true.

◆ name
   Specifies a unique name for the component.

◆ patching-type
   Specifies whether this resource provides minimal or full path patching.

◆ path-match-case
   Specifies whether the application URI is case-sensitive. The default value is true.

◆ proxy-host
   Specifies the proxy host that the portal access uses. The default value is none. If you configure this option, you must also configure the option proxy-port.

◆ proxy-port
   Specifies the port that the portal access proxy uses. The default value is none. Configure this option, only when you configure the option proxy-host.

◆ publish-on-webtop
   Specifies whether to publish this resource on the webtop. The default value is false. If you set this option to true, you must also specify the Application URI using the application-uri option.

◆ scheme-patching
   Specifies whether this resource replaces all HTTP scheme addresses with HTTPS scheme addresses. This option is effective only when minimal patching is selected for patching-type. The default value is false.
See also

apm, create, delete, edit, list, modify, show, tmsh
webtop

Configures a webtop resource.

Module

apm resource

Syntax

Configure the webtop component within the resource module using the syntax shown in the following sections.

Create/Modify

create webtop [name]
modify webtop [name]

options:
  customization-group [string]
  description [string | none]
  minimize-to-tray [false | true]
  portal-access-start-uri [string | none]
  webtop-type [full | last | network-access | portal-access]

edit webtop [ [name] | [glob] | [regex] ] ... ]

options:
  all-properties
  non-default-properties

Display

list webtop
list webtop [ [name] | [glob] | [regex] ] ... ]
show running-config webtop
show running-config webtop [ [name] | [glob] | [regex] ] ... ]

options:
  all-properties
  non-default-properties
  one-line

show webtop
show webtop [name]

Delete

delete webtop [name]
Description

Configures the settings necessary to define the webtop assigned to the end-user as part of the access policy execution.

Examples

Creates a webtop named `mynawebtop` with the customization group `mywebtopcg1` and the network access `minimize-to-tray` option set to false:

```plaintext
create webtop mynawebtop { customization-group mywebtopcg1 minimize-to-tray false }
```

Creates a webtop named `mywawebtop` with the customization group `mywebtopcg1` and the starting URI for the portal access of `http://www.siterequest.com`:

```plaintext
create webtop mywawebtop { customization-group mywebtopcg1 portal-access-start-uri "http://www.siterequest.com" }
```

Options

You can use these options with the `webtop` component:

- **customization-group**
  
  Specifies the customization settings for the webtop.

  *Note: You must create a customization group of type `webtop` before you can create a webtop resource. This option is required.*

- **description**
  
  Specifies a description of the resource. The default value is `none`.

- **portal-access-start-uri**
  
  Specifies the URI that the webtop starts. You can only configure this option if you have configured the `webtop-type` option for `portal-access`.

- **minimize-to-tray**
  
  Specifies whether the network access window (launched from the full webtop) is minimized to the system tray automatically after the network access connection starts. The default value is `true`.

  You can configure this option only if you configured the `webtop-type` option as `network-access` or `full`. With a network access webtop, the webtop automatically minimizes to the tray. With a full webtop, the webtop minimizes to the system tray only after the network access connection is started.

- **webtop-type**
  
  Specifies the type of webtop this resource creates.

  The options are:

  - **full**
    
    A webtop to which you assign a single network access resource, multiple portal access resources, and multiple application access app tunnel resources, or any combination of the three types. This is the default.
Chapter 11

- last
- network-access
  A webtop to which you assign only a single network access resource.
- portal-access
  A webtop to which you assign only portal access resources.

See also

apm, create, delete, edit, list, modify, show, tmsh
webtop-link

Configures a webtop link resource.

Module

apm resource

Syntax

Configure the webtop-link component within the resource module using the syntax shown in the following sections.

Create/Modify

create webtop-link [name]
modify webtop-link [name]
  options:
    application-uri [string]
    customization-group [string]
    description [[string] | none]
edit webtop-link [ [ [name] | [glob] | [regex] ] ... ]
  options:
    all

Display

list webtop-link
list webtop-link [ [ [name] | [glob] | [regex] ] ... ]
show running-config webtop-link
show running-config webtop-link [ [ [name] | [glob] | [regex] ] ... ]
  options:
    all-properties
    non-default-properties
    one-line
show webtop-link
show webtop-link [name]

Delete

delete webtop-link [name]
Description

Configures the settings necessary to define a link to a webtop that is displayed to the end-user as part of the access policy execution.

Examples

Creates a webtop named `mywebtoplinkcg1` with the application-uri of `http://www.externalsite.com/`:

```
cREATE WEBTOP-LINK MYWEBTOPLINKCG1 APPLICATION-URI "http://www.externalsite.com/"
```

Options

You can use these options with the `webtop-link` component:

- **application-uri**
  Specifies the application URI of the external portal to which this resource provides access for this webtop link. This is a required setting.

- **customization-group**
  Specifies the customization settings for the webtop.
  
  **Note**: You must create a customization group of type `webtop` before you can create a webtop resource. If you do not specify a customization group, a group will be created automatically.

- **description**
  Specifies a description of the resource. The default value is `none`.

See also

`apm`, `create`, `delete`, `edit`, `list`, `modify`, `show`, `tmsh`
apm resource remote-desktop Module Components

- Introducing the apm resource remote-desktop module
- Alphabetical list of components
Introducing the apm resource remote-desktop module

You can use the tmsh components that reside within the apm resource remote-desktop module to configure BIG-IP® Access Policy Manager®. For more information about the tmsh hierarchical structure, see Chapter 2, Understanding and Using the Traffic Management Shell.

Alphabetical list of components

The remainder of this chapter lists the tmsh components that are available in the apm resource remote-desktop module.
citrix

Configures a Citrix® remote desktop resource configuration object.

Module

apm resource remote-desktop

Syntax

Configure the citrix component within the resource remote desktop module using the syntax shown in the following sections.

Create/Modify

create citrix [name]
modify citrix [name]

options:
    acl-order [[integer] | none]
    auto-logon [enabled | disabled]
    customization-group [add | delete | modify | replace-all-with] {
        [name] {
            options:
                caption [[string] | none]
                detailed-description [[string] | none]
        }
    }
    description [[string] | none]
    domain-source [session.logon.last.domain | none]
    enable-serverside-ssl [enabled | disabled]
    host [fqdn]
    ip [ip address]
    log [config | none | packet | summary | verbose]
    password-source [session.logon.last.password | none]
    port [[string] | none]
    username-source [session.logon.last.username | none]

edit citrix [ [ [name] | [glob] | [regex] ] ... ]

options:
    all-properties
    non-default-properties
Display

```
list citrix
list citrix [ [name] | [glob] | [regex] ] ... ]
show running-config citrix
show running-config citrix [ [name] | [glob] | [regex] ] ... ]
  options:
    all-properties
    non-default-properties
show citrix
show citrix [name]
```

Delete

```
delete citrix [name]
```

Description

You can use the `citrix` component to configure a Citrix remote desktop resource.

Examples

```
Creates a Citrix remote desktop resource named `mycitrix` with an IP address of 172.29.67.130:

create citrix mycitrix { host 172.29.67.130 customization-group my_citrix_customization }

Creates a Citrix resource with Citrix server of 172.29.67.130 and auto-logon enabled with APM credentials (that user types on Logon Page):

create citrix my { host 172.29.67.130 customization-group my_citrix_customization
  auto-logon enabled }

Creates a Citrix resource with Citrix server of 172.29.67.130 and SSL communication enabled to that server (SSL should also be enabled on the server):

create citrix my { host 172.29.67.130 customization-group my_citrix_customization
  enable-serverside-ssl enabled }
```

Options

You can use these options with the `citrix` component:

- **acl-order**
  Specifies the order in which you want the Citrix server to appear in the ACL Order list. The default value is 0 (zero).
◆ **auto-logon**
   Enables or disables automatic log on to the Citrix server. If you enable this option, you must also provide values for the **username-source**, **password-source**, and **domain-source** options. The default value is disabled.

◆ **customization-group**
   Specifies whether customization groups are applied to the Citrix remote desktop. You can add, modify, or delete customization groups. You can also replace all current customization groups with new customization groups. The default value is none.

◆ **description**
   Specifies a description for your Citrix remote desktop. The default value is none.

◆ **domain-source**
   Specifies the Session variable used as a source for the **auto-logon** user password. The default value is `session.logon.last.domain`.

◆ **enable-serverside-ssl**
   Enables or disables SSL capabilities between the BIG-IP system and the Citrix server. When enabled, the port number automatically changes to 443. The default value is disabled.

◆ **host**
   Specifies the hostname of your Citrix server. Either the `host` or `ip` option is required; however, you cannot specify both options.

◆ **ip**
   Specifies the IP address of your Citrix server. Either the `host` or `ip` option is required; however, you cannot specify both options.

◆ **log**
   Specifies the log format. The default value is none.
   The options are:
   - **config**
   - **none**
     The system does not log packets sent to and from the Citrix server.
   - **packet**
     The system logs packets sent to and from the Citrix server.
   - **summary**
     The system provides a short summary of the communications between the BIG-IP system and the Citrix server.
   - **verbose**
     The system provides an extensive summary of the communications between the BIG-IP system and the Citrix server.

◆ **name**
   Specifies an object name. This option is required; however, the parameter name is implicit and must not be typed in the syntax.

◆ **password-source**
   Specifies the session variable that is used as a source for the **auto-logon** password. The default value is `session.logon.last.password`. 
apm resource remote-desktop Module Components

- **port**
  Specifies the port for your Citrix server. The default value is 80.

- **username-source**
  Specifies the session variable that is used as a source for the `auto-logon` user name. The default value is `session.logon.last.username`.

### See also

citrix-client-bundle, citrix-client-package-file, rdp
citrix-client-bundle

Configures a Citrix Client Bundle remote desktop resource configuration object.

Module

apm resource remote-desktop

Syntax

Configure the citrix-client-bundle component within the resource remote desktop module using the syntax shown in the following sections.

Create/Modify

create citrix-client-bundle [name]
modify citrix-client-bundle [name]
   options:
      download-url [url] | none
      packages [string] | none
      windows-download-url [url] | none
      windows-min-version [string] | none
      windows-package [string] | none
edit citrix-client-bundle [ [ [name] | [glob] | [regex] ] ... ]
   options:
      all-properties
      non-default-properties

Display

list citrix-client-bundle
list citrix-client-bundle [ [ [name] | [glob] | [regex] ] ... ]
show running-config citrix-client-bundle
show running-config citrix-client-bundle [ [ [name] | [glob] | [regex] ] ... ]
   options:
      all-properties
      non-default-properties
      one-line
      partition
show citrix-client-bundle
show citrix-client-bundle [name]
Delete

```
delete citrix-client-bundle [name]
```

Description

You can use the `citrix-client-bundle` component to configure a Citrix Client Bundle remote desktop resource.

Examples

Creates a Citrix Client Bundle remote desktop resource named `myccb` that can be downloaded from `www.citrix.com/download` (the default value), where the client must have at least Windows® XP installed:

```
create citrix-client-bundle myccb { windows-min-version xp }
```

Options

You can use these options with the `citrix-client-bundle` component:

- **download-url**
  Specifies the default location `www.citrix.com/download` from which to download the Citrix installation package.

- **packages**
  Specifies the location from which to download client installer package. The default value is `none`.

- **name**
  Specifies an object name. This option is required; however, the parameter `name` is implicit and must not be typed in the syntax.

- **windows-download-url**
  Specifies the location from which to download the Windows version. You can provide a value for either the `windows-download-url` or `windows-package` option, but not both. The default value is `none`.

- **windows-min-version**
  Specifies the oldest version of the Citrix client that can be used with this remote desktop resource. The default value is `none`.

- **windows-package**
  Specifies the location from which to download the Windows package. You can provide a value for either the `windows-package` or `windows-download-url` option, but not for both. The default value is `none`.

See also

`citrix`, `citrix-client-package-file`, `rdp`
citrix-client-package-file

Configures a Citrix client package file configuration object.

Module

apm resource remote-desktop

Syntax

Configure the **citrix-client-package-file** component within the **resource remote desktop** module using the syntax shown in the following sections.

Create/Modify

create citrix-client-package-file [name]
modify citrix-client-package-file [name]
options:
    original-file-name [[string] | none]
    source-path [[string] | none]
edit citrix-client-package-file [ [ [name] | [glob] | [regex] ] ... ]
options:
    all-properties
    non-default-properties

Display

list citrix-client-package-file
list citrix-client-package-file [ [ [name] | [glob] | [regex] ] ... ]
show running-config citrix-client-package-file
show running-config citrix-client-package-file [ [ [name] | [glob] | [regex] ] ... ]
options:
    all-properties
    non-default-properties
    one-line
    partition

Delete

delete citrix-client-package-file [name]

Description

You can use the **citrix-client-package-file** component to configure access to a Citrix client package file.
Examples

Creates a Citrix client package remote desktop resource named `myccpackage` that is available from `www.siterequest.citrix_download.com`:

```bash
create citrix-client-package myccpackage {
    source-path www.siterequest.citrix_download.com
}
```

Options

You can use these options with the `citrix-client-package` component:

- **name**
  Specifies an object name. This option is required; however, the parameter `name` is implicit and must not be typed in the syntax.

- **original-file-name**
  Specifies the original file name of the Citrix Installation package file name to download. The default value is `none`.

- **source-path**
  Specifies the location from which to download the Citrix client package file. This option is required.

See also

`citrix, citrix-client-package-file, rdp`
rdp

Configures a Microsoft® Remote Desktop Protocol (RDP) configuration object.

Module

apm resource remote-desktop

Syntax

Configure the rdp component within the resource remote desktop module using the syntax shown in the following sections.

Create/Modify

create rdp [name]
modify rdp [name]

options:
  acl-order [integer | none]
  application [string | none]
  auto-logon [enabled | disabled]
  color-depth [4 | 8 | 16 | 24]
  customization-group [add | delete | modify | replace-all-with] {
    [name] {
      options:
        caption [string | none]
        detailed-description [string | none]
    }
  }
  description [string | none]
  domain-source [session.logon.last.domain | none]
  host [fqdn]
  ip [ip address]
  java-client [enabled | disabled]
  log [config | none | packet | summary | verbose]
  password-source [session.logon.last.password | none]
  port [[integer] | none]
  rdp-cache-bitmaps [true | false]
  rdp-show-contents-while-dragging [true | false]
  rdp-show-desktop-wallpaper [true | false]
  rdp-show-themes [true | false]
  rdp-window-animations [true | false]
  redirect-com-parts [true | false]
redirect-drives [true | false]
redirect-keyboard-commands [true | false]
redirect-printers [true | false]
redirect-sound [true | false]
username-source [session.logon.last.username | none]
window-height [[integer] | none]
window-percent-of-desktop [[integer] | none]
window-size [custom-size | full-screen | percent-of-desktop | seamless]
window-width [[integer] | none]
work-dir [[string] | none]
edit rdp [ [ [name] | [glob] | [regex] ] ... ]
    options:
    all-properties
    non-default-properties

Display

list rdp
list rdp [ [ [name] | [glob] | [regex] ] ... ]
show running-config rdp
show running-config rdp [ [ [name] | [glob] | [regex] ] ... ]
    options:
    all-properties
    non-default-properties
show rdp
show rdp [name]

Delete

delete rdp [name]

Description

You can use the rdp component to configure a Microsoft RDP resource.

Examples

Creates an RDP resource named myrdp with an RDP server with an IP address of 172.29.67.130:

create rdp myrdp { host 172.29.67.130 }

Creates an RDP resource named myrdp with an RDP server with an IP address of 172.29.67.130 where bitmaps are cached on the client PC:

create rdp myrdp { host 172.29.67.130 rdp-cache-bitmaps true }
Options

You can use these options with the rdp component:

- **acl-order**
  Specifies the order in which you want the RDP server to appear in the ACL Order list. The default value is 0 (zero).

- **application**
  Specifies the executable name of the application, for example notepad.exe. You can include the full path to the application, for example "C:\my\mybinary.exe".

- **auto-logon**
  Specifies if automatic log on to the Microsoft RDP server is used. If you enable this option, you must also provide values for the username-source, password-source, and domain-source options. The default value is disabled.

- **color-depth**
  Specifies the requested remote session color depth. The default value is 32.

  The options are:
  - 24-bit
  - 16-bit
  - 8-bit
  - 4-bit

- **customization-group**
  Specifies whether customization-groups are applied to the remote desktop. You can add, modify, delete, or replace all customization-groups. The default value is none.

- **description**
  Specifies a description of an RDP resource. The default value is none.

- **domain-source**
  Specifies the session variable used as a source for the auto-logon user password. The default value is session.logon.last.domain.

- **host**
  Specifies the hostname of your Microsoft RDP server. Either the host or ip option is required; however, you cannot specify both options.

- **ip**
  Specifies the IP address of your Microsoft RDP server. Either the host or ip option is required; however, you cannot specify both options.

- **java-client**
  Specifies if JavaScript™ is enabled or disabled on the client. The default value is enabled.
◦ **log**
  Specifies the log format. The default value is **none**.
  The options are:
  - **config**
  - **none**
    The system does not log packets sent to and from the Microsoft RDP server.
  - **packet**
    The system logs packets sent to and from the Microsoft DP server.
  - **summary**
    The system provides a short summary of the communications between the BIG-IP system and the Microsoft RDP server.
  - **verbose**
    The system provides an extensive summary of the communications between the BIG-IP system and the Microsoft RDP server.

◦ **name**
  Specifies an object name. This option is required; however, the parameter **name** is implicit and must not be typed in the syntax.

◦ **password-source**
  Specifies the session variable used as a source for the **auto-logon** password. The default value is **session.logon.last.password**.

◦ **port**
  Specify port **3389** for your Microsoft RDP server. The default value is **0** (zero).

◦ **rdp-cache-bitmaps**
  Specifies whether to cache bitmap files on the client. The default value is **true**.

◦ **rdp-show-contents-while-dragging**
  Specifies whether to show the contents of a window when the user is dragging the window. The default value is **false**.

◦ **rdp-show-desktop-wallpaper**
  Specifies whether to display the desktop background. The default value is **false**.

◦ **rdp-show-themes**
  Specifies whether to display the desktop theme. The default value is **false**.

◦ **rdp-window-animations**
  Specifies whether to display Window animations. The default value is **false**.

◦ **redirect-com-ports**
  Specifies whether to connect to your communication ports. The default value is **false**.

◦ **redirect-drives**
  Specifies whether to connect to your local drives. The default value is **false**.
◆ **redirect-keyboard-commands**
   Specifies when to redirect keyboard commands to a remote session. When enabled, commands such as Alt-tab and Ctrl-Alt-Del are available in remote sessions. The default value is **in-full-screen**.

   The options are:
   - **enable**
     The keyboard commands for the remote desktop are available to the user.
   - **disable**
     The keyboard commands for the remote desktop are not available to the user.
   - **in-full-screen**
     The keyboard commands for the remote desktop are available to the user only when the value of the **window-size** option is **full-screen**.

◆ **redirect-printers**
   Enables or disables connection to a local printer. The default value is **disabled**.

◆ **redirect-sound**
   Enables or disables sounds playing in a remote session. The default value is **disabled**.

◆ **username-source**
   Specifies the session variable used as a source for the auto-logon user name. The default value is **session.logon.last.username**.

◆ **window-height**
   Specifies the height, in pixels, of the remote desktop window. Set this option only when you set the value of the **window-size** option to **custom**. The default value is 600 pixels.

◆ **window-percent-of-desktop**
   Specifies the width and height of the remote session window as a percentage of the user’s desktop.

◆ **window-size**
   Specifies the type of window sizing to use on the client desktop. The default value is **custom-size**.

   The options are:
   - **full-screen**
     The remote desktop window fills the entire screen.
   - **percent-of-desktop**
     The value you configure represents a percentage of the screen that the remote desktop fills.
   - **custom**
     When you use this option, you must also set the **window-height** and **window-width** options.
   - **seamless**

◆ **window-width**
   Specifies the width, in pixels, of the remote desktop window. The default value is 800 pixels.
**workdir**
Specifies the directory you want the user to access on the target server.
The default value is **none**.

See also

citrix, citrix-client-bundle, citrix-client-package-file
apm sso Module Components

• Introducing the apm sso module
• Alphabetical list of components
Introducing the apm sso module

You can use the tmsh components that reside within the apm sso module to configure BIG-IP® Access Policy Manager®. For more information about the tmsh hierarchical structure, see Chapter 2, Understanding and Using the Traffic Management Shell.

Alphabetical list of components

The remainder of this chapter lists the tmsh components that are available in the apm sso module.
basic

Configures a single sign-on (SSO) HTTP basic authentication configuration object.

Module

apm sso

Syntax

Configure the basic component within the sso module using the syntax shown in the following sections.

Create/Modify

create basic [name]
modify basic [name]
options:
  headers [add | delete | modify | | replace-all-with] {
    [name] {
      options:
        hname [[URL] | none]
        hvalue [[integer] | none]
    }
  }
  password-source [session.sso.token.last.password | none]
  username-conversion [enabled | disabled]
  username-source [session.sso.token.last.username | none]
edit basic [ [ [name] | [glob] | [regex] ] ... ]
options:
  all-properties
  non-default-properties

Display

list basic
list basic [ [ [name] | [glob] | [regex] ] ... ]
show running-config basic
show running-config basic [ [ [name] | [glob] | [regex] ] ... ]
options:
  all-properties
  non-default-properties
  one-line
  partition
show basic
show basic [name]

Delete

delete basic [name]

Description

You can use the basic component to create, modify, display, or delete an SSO HTTP basic authentication configuration object.

Examples

Creates an SSO basic configuration object named mybasic:

```
create basic mybasic
```

Options

You can use these options with the basic component:

- **headers**
  Specifies the name and value of the HTTP header content to be inserted in an HTTP Request that passes through the **apm sso** module. The default value is **none**.
  The options are:
  - **hname**
    The name of the HTTP header.
  - **hvalue**
    The value of the HTTP header.
- **name**
  Specifies a name for the SSO configuration. This option is required.
- **partition**
  Displays the partition in which the object resides.
- **password-source**
  Specifies the source from which you want SSO to retrieve the password to use to authenticate applications.
- **username-conversion**
  Enables or disables conversion of PREWIN2K/UPN user name input format to the format for SSO to use. The default value is **disabled**.
- **username-source**
  Specifies the source from which you want SSO to retrieve the user name to use to authenticate applications.
See also

apm, create, delete, edit, list, modify, show, tmsh
form-based

Configures an SSO form-based configuration object.

Module

apm sso

Syntax

Configure the form-based component within the sso module using the syntax shown in the following sections.

Create/Modify

create form-based [name]
modify form-based [name]

options:
  form-action [[URL] | none]
  form-field [string]
  form-method [get | post]
  form-password [string]
  form-username [string]
  headers [add | delete | modify | | replace-all-with] {
    [name] {
      options:
        hname [[URL] | none]
        hvalue [[integer] | none]
    }
  }
  password-source [session.sso.token.last.password | none]
  start-uri [[URLs] | none]
  success-match-type [cookie | none | url]
  success-match-value [string]
  username-source [session.sso.token.last.username | none]

edit form-based [ [ [name] | [glob] | [regex] ] ... ]

options:
  all-properties
  non-default-properties
Chapter 13

Display

list form-based
list form-based [ [ [name] | [glob] | [regex] ] ... ]
show running-config form-based
show running-config form-based [ [ [name] | [glob] | [regex] ] ... ]

options:
all-properties
non-default-properties
one-line
partition
show form-based
show form-based [name]

Delete

delete form-based [name]

Description

You can use the form-based component to configure an SSO form-based configuration object.

Examples

Creates an SSO form-based configuration object named fb_2011_sso:

create form-based fb_2011_sso { start-uri
"/fb/auth/logon.aspxurl=https://exch2011.mv1.fp.com/fp/&reason=0" form-action
"/fp/auth/fpauth.dll" form-username "username" form-password "password" form-field
*destination https://exch2011.mv1.fp.com/fp/&#34; }

Options

You can use these options with the form-based component:

◆ form-action
  Specifies the form action URL that is used for HTTP form-based authentication. This is optional. If you do not specify a form action, then Access Policy Manager uses the URI from the request to perform HTTP form-based authentication. The default value is none.

◆ form-field
  Specifies the hidden form parameters that are required by the authentication server logon form at your location. Refer to the BIG-IP® Access Policy Manager® Single Sign-On Configuration Guide for more information on how to determine hidden values. The default value is none.
◆ **form-method**
   Specifies the form method to use for form-based HTTP authentication. The value is either `get` or `post`. The default value is `post`. If you specify `get`, Access Policy Manager forces the authentication using HTTP GET rather than authenticating using form-based POST.

◆ **form-password**
   Specifies the parameter names used by the form that is sent the POST request.

◆ **form-username**
   Specifies the parameter names used by the form that is sent the POST request.

◆ **headers**
   Specifies the name and value of the HTTP header content to be inserted in an HTTP Request that passes through the APM™ SSO module. The default value is `none`.
   The options are:
   - **hname**
     Specifies the name of the HTTP header.
   - **hvalue**
     Specifies the value of the HTTP header.

◆ **name**
   Specifies a name for the component.

◆ **password-source**
   Specifies the password you want cached for single sign-on. The default value is `session.sso.token.last.password`.

◆ **start-uri**
   Specifies a URL resource. For example, for FB, it would be `/fb/auth/logon.aspx`. For Citrix, `/Citrix/XenApp/auth/logon.aspx`. This resource must respond with a challenge to a non-authenticated request. The default value is `none`.

◆ **success-match-type**
   Specifies the method your authentication server uses. If you specify a value for this option, you must also specify a value for `success-match-value`. The default value is `none`.
   The options are:
   - **url**
     One or more URLs. The system supports only the wildcard character (*).
   - **cookie**
     A cookie name.

◆ **success-match-value**
   Specifies the value used to specify either the URL(s) or cookie for the `success-match-type` option. The default value is `none`.

◆ **username-source**
   Specify the user name you want cached for single sign-on. The default value is `session.sso.token.last.username`.
See also

sso basic, sso kerberos, sso ntlmv1, sso ntlmv2
form-basedv2

Configures an SSO form-basedv2 configuration object.

Module

apm sso

Syntax

Configure the form-basedv2 component within the sso module using the syntax shown in the following sections.

Create/Modify

create form-basedv2 [name] {
  forms [add | replace-all-with] {
    [name] {
      request-value [URIs]
      controls [add | replace-all-with] {
        [name] {
          value [string]
        }
      }
    }
  }
}

modify form-basedv2 [name]

  options:
    forms [add | delete | modify | replace-all-with] {
      [name] {
        options:
          attribute-value [[string] | none]
          controls [add | delete | modify | replace-all-with] {
            [name] {
              options:
                secure [true | false]
                value [string]
            }
          }
    }
    description [[string] | none]
    form-order [integer]
    id-type [action | id | inputs | name | order]
    request-method [get | post]
request-name [[string] | none]
request-negative [true | false]
request-prefix [true | false]
request-type [cookie | header | uri]
request-value [[string] | none]
submit-autodetect [true | false]
submit/javascript [[string] | none]
submit/javascript-type [auto | custom | extra]
submit-method post
submit-name [[string] | none]
submit-negative [true | false]
submit-prefix [true | false]
submit-type [cookie | header | uri]
submit-value [[string] | none]
success-match-type [cookie | none | url]
success-match-value [[string] | none]
}
}
headers [add | delete | modify | none | replace-all-with] {
 [name] {
  options:
  description [[string] | none]
  name [string]
  value [string]
 }
}
log-level [alert | crit | debug | emerg | err | info | notice | warn]
edit form-basedv2 [ [[name] | [glob] | [regex] ] ... ]
  options:
  all-properties
  non-default-properties
reset-stats
reset-stats [ [[name] | [glob] | [regex] ] ... ]

Display
list form-basedv2
list form-basedv2 [ [[name] | [glob] | [regex] ] ... ]
show running-config form-basedv2
show running-config form-basedv2 [ [[name] | [glob] | [regex] ] ... ]
  options:
  all-properties
  non-default-properties
  one-line
You can use the `form-basedv2` component to configure an SSO form-based v2 configuration object. When creating a new SSO form-basedv2 configuration object, you must add at least one `forms` item and, within it, at least one `controls` item. You must also provide a value for the `request-value` option in the `forms` item.

The SSOv2 module identifies and processes two types of application HTTP requests - logon page requests and credentials submit requests. Logon page requests are identified using the `request`- set of options. Credentials submit requests, in most cases, are identified automatically. When this fails, you can set the `submit-autodetect` option to `false` and use the `submit`- set of options to identify these requests.

When the SSOv2 module identifies a logon page request, it scans the response trying to find the logon form. If the logon form is found, SSOv2 inserts a JavaScript code that will cause the logon form to be submitted automatically by the browser. The client must support JavaScript.

When the SSOv2 module identifies a credentials submit request, it compares POST data parameter names with form controls defined in the configuration. For a POST data parameter name that has a corresponding form control, the SSOv2 module replaces its value with the control value from the configuration. Control values are usually supplied through session variables, such as `session.sso.token.last.username` and `session.sso.token.last.password`. POST data parameters that have no corresponding controls in the configuration are not changed.

The majority of web applications have a single logon page with one logon form. You will need to define a single `forms` item for these applications. In rare cases when an application has multiple logon pages with different logon forms, you will need to create multiple `forms` items, one for each logon page/form. If multiple logon pages use the same form, you will need only one `forms` item with a list of URIs for all logon pages.

Every `forms` item must include at least one `controls` item, and can include up to 32 `controls` items. Each `controls` item represents an input element of an HTML logon form, such as form fields for entering user name and password, and, optionally, any hidden form parameters. The name of the `controls` item must match the name attribute of the corresponding input tag of the form. For example, if the form has the following HTML tag for entering the user name, the `forms` item must include a `controls` item with the name `Bugzilla_login`:

```html
<input id="Bugzilla_login_top"
class="bz_login"
```
The `controls` item used for entering the user's password must have the `secure` option set to `true`. The value of a control item should usually be the name of a session variable, starting with the percent (%) sign and enclosed in braces ({ }); for example, the value for the user name control item: `{{session.sso.token.last.username}}`. The value can also be a string, or a combination of strings and session variable names.

### Examples

Creates an SSO form-basedv2 configuration object named `fbssov2-owa2010`:

```
create form-basedv2 fbssov2-owa2010 { forms add { owa2010 { controls add { password { secure true value \{{session.sso.token.last.password\} \} username { value \{{session.sso.token.last.username\} \} request-value /owa/auth/logon.aspx?replaceCurrent=1 submit-javascript clkLgn() submit-javascript-type extra success-match-type cookie success-match-value sessionid } } }}>
```

Deletes an SSO form-basedv2 configuration object named `fbssov2-owa2010`:

```
delete fbsso-owa2010
```

### Options

You can use these options with the form-basedv2 component:

- **forms**
  - Specifies one or more items, each defining SSO processing of a separate application logon form.
  - **[name]**
    - Specifies the name of the form item. It does not have to match the actual name of the HTML form and can be arbitrary.
    - The options are:
      - **attribute-value**
        - Specifies the value of the HTML form tag attribute used to identify the logon form. The attribute could be `id`, `name`, or `action`, and is specified by the `id-type` option. For other values of the `id-type` option, this is not used and should be set to `none`.
      - **controls**
        - Specifies one or more form control items (up to 32) that you want to be processed by SSOv2.
      - **[name]**
        - Specifies the name of the HTML form control item. It must match the name attribute value of the HTML form's input tag.
        - The options are:
• **secure**
  Specifies whether the control item represents the HTML input tag
  of type "password". The default is **false**.

• **value**
  Specifies the value of the control item. This is usually the name of
  a session variable. If the session variable is not found when the
  SSO request is processed, the value of the corresponding POST
  parameter will be empty. The value could also be a literal string or
  a combination of strings and session variable names.

◆ **description**
  User-defined description.

◆ **form-order**
  Specifies the order of the HTML logon form on the logon page when the
  **id-type** option is set to **order**. Starts with 1.

◆ **headers**
  Specifies the name and value of the HTTP header to be inserted in an
  HTTP Request that passes through the APM SSOv2 module.

  • **[name]**
    Specifies the name of the headers item.
    The options are:
    • **name**
      Specifies the name of the HTTP header.
    • **value**
      Specifies the value of the HTTP header.

◆ **id-type**
  Specifies how the HTML logon form is found in the HTML body of the
  logon page. If there is more than one form on the logon page matching
  the criteria, the first match is used. The default is **inputs**.
  The options are:
  • **action**
    The logon form is identified by the value of the **form** tag in the **action**
    attribute. The value is specified in the **attribute-value** option.
  • **id**
    The logon form is identified by the **id** attribute's value of the **form**
    tag. The value is specified in the **attribute-value** option.
  • **name**
    The logon form is identified by the **name** attribute's value of the **form**
    tag. The value is specified in the **attribute-value** option.
  • **order**
    The logon form is identified by its relative order on the logon page
    (starting from 1). The order is specified in the **form-order** option.
  • **inputs**
    The logon form is identified by a combination of **controls** items. The
    controls in the configuration must have corresponding **input** elements
    in the form.
◆ log-level
  Specifies the log level. Valid values are alert, crit, debug, emerg, err, info, notice, warn. The default is notice.

◆ request-method
  Specifies the HTTP method of the application's request returning logon page. Default is get.

◆ request-name
  Specifies the name of the HTTP cookie or the name of the HTTP header used to identify application's request for logon page. The cookie or header is selected by the request-type option. The value of the cookie or header is specified by the request-value option. When the request-type option is set to uri, this option is not used and should be set to none.

◆ request-negative
  When set to true, the application's request for logon page will be identified by the absence of the specified cookie or header, or by a failed match against the list of specified URIs. The default is false.

◆ request-prefix
  Specifies how the value of the request-value option will be used to match one of the HTTP request cookie, header, or URI. The default is true and specifies a partial match; false specifies an exact match.

◆ request-type
  Specifies which element of the HTTP request headers is used to identify the application's request for logon page. The default is uri.
  The options are:
  • cookie
    The request is identified by the presence (or absence) of a cookie. The name and value of the cookie are specified by the request-name and request-value options.
  • header
    The request is identified by the presence (or absence) of the HTTP header. The name and value of the header are specified by the request-name and request-value options.
  • uri
    The request is identified by a successful (or failed) match against a list of URIs specified by the request-value option, and the request-name option is not used.

◆ request-value
  Specifies the value of the HTTP request element that must be matched to identify the request as the application's request for the logon page. This is one of: the cookie value, the header value, or a list of URIs (one per line) as specified by the request-type option. Cookie or header value could be set to none, in which case only the presence of the named cookie or header is checked and the value is not checked. When checking for URI, the value must be specified.
submit-autodetect
When set to true, the application's HTTP request that submits the user's credentials will be identified automatically and other submit- options should not be used. When false, the form submit will be identified using a combination of other submit-options. The default is true.

submit-javascript
Specifies user-provided JavaScript code to be inserted into the logon page to perform automatic form submission when the submit-javascript-type option is set to custom. The custom JavaScript code replaces the code automatically generated by the SSOv2 module. When the submit-javascript-type option is set to extra, it specifies the application's JavaScript functions to call from the automatically generated JavaScript code prior to submitting a logon form. When the submit-javascript-type option is set to auto, this option should be set to none.

submit-javascript-type
Specifies the type of JavaScript code to be inserted into the logon page by the SSOv2 module to perform automatic logon form submission. The options are:

- auto
  JavaScript code is automatically generated by the SSOv2 module.

- custom
  JavaScript code is provided by the user in the submit-javascript option.

- extra
  JavaScript code is automatically generated by the SSOv2 module, and additional JavaScript code provided by the user in the submit-javascript option is inserted before the form submit statement.

submit-method
Specifies the HTTP method of credentials submit request for the application. This must be set to post. This option is not used when submit-autodetect is true.

submit-name
Specifies the name of the HTTP cookie or the name of HTTP header used to identify credentials submit request for the application. The cookie or header is selected by the submit-type option. The value of the cookie or header is specified by the submit-value option. When the submit-type option is set to uri, this option is not used and should be set to none. This option is not used when submit-autodetect is true.

submit-negative
When set to true, the credentials submit request for the application is identified by the absence of a specified cookie or header, or by a failed match against the list of specified URIs. The default is false. This option is not used when submit-autodetect is true.
◆ submit-prefix
Specifies how the value of the submit-value option will be used to match the HTTP request cookie, header, or URI. The default is true and specifies partial match; false specifies exact match. This option is not used when submit-autodetect is true.

◆ submit-type
Specifies which element of HTTP request headers is used to identify the credentials submit request for the application. The default is uri. This option is not used when submit-autodetect is true.
The options are:
• cookie
    The request is identified by the presence (or absence) of a cookie. The name and value of the cookie are specified by the submit-name and submit-value options.
• header
    The request is identified by the presence (or absence) of the HTTP header. The name and value of the header are specified by the submit-name and submit-value options.
• uri
    The request is identified by a successful (or failed) match against a list of URIs specified by the submit-value option and the submit-name option is not used.

◆ submit-value
Specifies the value of the HTTP request element that must be matched to identify the request as a credentials submit request for the application. This is one of: the cookie value, the header value, or a list of URIs (one per line) as specified by the submit-type option. Cookie or header value could be set to none, in which case only the presence of the named cookie or header is checked and the value is not checked. When checking for URI, the value must be specified. This option is not used when submit-autodetect is true.

◆ success-match-type
Specifies how the SSOv2 module detects whether the credentials submit request was successful. When the SSOv2 module detects that the credentials submission failed, the SSOv2 configuration used for this HTTP transaction is disabled for the user session. If you specify a value for this option, you must also specify a value for success-match-value. The default is none.
The options are:
• url
    Credentials submission was successful if the response contains the HTTP Location header with a value matching one of the URLs specified by the success-match-value option.
• cookie
    Credentials submission was successful if the response contains the HTTP cookie with the name specified by the success-match-value option.
• **none**
  No check is performed. If SSO logon fails and the application server redirects back to the logon page that matches the criteria of the logon page request, SSO will be retried, possibly causing an authentication loop.

• **success-match-value**
  Specifies the value used to detect the success or failure of the SSO logon. When the `success-match-type` option is set to `url`, this is a list of URLs. Each URL in the list can contain a single wildcard character (*). When the `success-match-type` option is set to `cookie`, this option specifies the name of the cookie. The default is `none`.

**See Also**

`sso basic`, `sso kerberos`, `sso ntlmv1`, `sso ntlmv2`, `sso form-based`
kerberos

Configures a Kerberos configuration object.

Module

apm sso

Syntax

Configure the kerberos component within the sso module using the syntax shown in the following sections.

Create/Modify

create kerberos [name]
modify kerberos [name]
options:
  account-name [string]
  account-password [string]
  app-service [[string] | none]
  headers [add | delete | modify | replace-all-with] {
    [name] {
      options:
        app-service [[string] | none]
        hname [[string] | none]
        hvalue [[integer] | none]
    }
  }
  kdc [[string] | none]
  realm [string]
  send-authorization [401 | always]
  spn-pattern [[string] | none]
  ticket-lifetime [[integer] | none]
edit kerberos [ [ [name] | [glob] | [regex] ] ... ]
options:
  all-properties
  non-default-properties

Display

list kerberos
list kerberos [ [ [name] | [glob] | [regex] ] ... ]
show running-config kerberos
show running-config kerberos [ [name] | [glob] | [regex] ] ...

options:

  all-properties
  non-default-properties
  one-line
  partition
show kerberos
show kerberos [name]

Delete

delete kerberos [name]

Description

You can use the kerberos component to configure an SSO Kerberos configuration object. Kerberos is an authentication protocol, where both the user and the server verify the other's identity.

Examples

Creates an SSO kerberos configuration object named mykerberos for the realm myrealm.com, where the account name is apmaccount and the password is ****:

create mykerberos { realm MYREALM.COM account-name apmaccount account-password **** }

Options

You can use these options with the kerberos component:

  ◆ account-name
  Specifies the name of the Active Directory® (AD) account configured for delegation. This account must be configured in the server's Kerberos realm (AD Domain). If servers are from multiple realms, each realm (AD Domain) must have its own delegation account. This option is required.

  ◆ account-password
  Specifies the password for the delegation account specified in account-name. This option is required.

  ◆ headers
  Specifies custom HTTP headers to insert into a request. The default value is none.
  The options are:
    ◆ hname
    Specifies the name of a header to add to a request.
• **hvalue**
  Specifies the value of a header to add to a request.

• **kdc**
  Specifies the IP Address or host name of the Kerberos Key Distribution Center (KDC) for the server's realm. This is normally an Active Directory domain controller. If you leave this empty, the KDC must be discoverable through DNS, for example, BIG-IP system must be able to fetch SRV records for the server realm's domain. If the server realm's domain name is different from the server's realm name, you must specify the server realm's domain name in the `/etc/krb5.conf` file. Kerberos SSO processing is fastest when KDC is specified by its IP address, slower when specified by host name, and even slower (due to additional DNS queries) when left empty. When a user's realm is different from server's realm, the KDC value must be empty. This is true in cases of cross-realm SSO. The default value is `none`.

• **name**
  Specifies the name for the SSO Kerberos configuration object. This option is required.

• **realm**
  Specifies the realm of application server(s), for example, pool members or portal access resource hosts. If the servers are located in multiple realms, each realm requires a separate SSO configuration. You must specify the realm in uppercase letters. The user's realm can be specified through the `session.logon.last.domain` session variable, and if this variable is not set, then the user's realm is assumed to be the same as the server's realm. This option is required.

• **send-authorization**
  Specifies when to submit a Kerberos ticket to the application server(s). The ticket is submitted in an HTTP Authorization header. The header value starts with the word `Negotiate`, followed by one space and a base64-encoded GSSAPI token containing the Kerberos ticket. If a request contains an Authorization header from the user's browser, it is deleted. The default value is `always`.
  
  The options are:
  - **401**
    The BIG-IP system first forwards the user's HTTP request to the web server without inserting a new Authorization header; however, the browser's Authorization header is deleted. If the server requests authentication by responding with a 401 status code, BIG-IP retries the request with the Authorization header. The Kerberos ticket GSSAPI representation uses the SPNEGO mechanism type (OID 1.3.6.1.5.5.2). Specifying **401** results in additional BIG-IP/server request round trips in case authentication is required for the request.
  - **always**
    The BIG-IP system inserts an Authorization header, including the Kerberos ticket, into every HTTP request, whether the request requires authentication or not. The Kerberos ticket GSSAPI representation uses the KRB5 Kerberos 5 mechanism type (OID
1.2.840.113554.1.2.2). Specifying always results in the additional overhead of generating a Kerberos token for every request. This is the default value.

◆ spn-pattern
Specifies how the Service Principal Name (SPN) for the server is constructed. For example, HTTP/%s@[server realm name configured in the realm option], where %s will be substituted with the hostname of your server discovered through reverse DNS lookup using the server IP address. Only specify this option when you need non-standard SPN format. The default value is none.

◆ ticket-lifetime
Specifies the lifetime of Kerberos tickets obtained for the user. The value represents the maximum ticket lifetime. The actual ticket lifetime can be less by up to 1 hour, because a user's ticket lifetime is the same as the Kerberos Ticket Granting Ticket (TGT) lifetime. A TGT is obtained for the delegation account specified in this configuration. A new TGT is fetched every time the current TGT is older than one hour. The new TGT can only be fetched when an SSO request is processed. The minimum ticket lifetime is 10 minutes. There is no maximum, however, the ticket lifetime of most AD domains is 10 hours (600 minutes). F5 Networks recommends that you set the ticket lifetime in an SSO configuration above what is specified in an AD domain. The default value is 600 minutes.

See also

sso basic, sso form-based, sso ntlmv1, sso ntlmv2
**ntlmv1**

Configures a single sign-on (SSO) NT LAN Manager, version 1 (ntlmv1) configuration object.

**Module**

apm sso

**Syntax**

Configure the ntlmv1 component within the sso module using the syntax shown in the following sections.

**Create/Modify**

create ntlmv1 [name]
modify ntlmv1 [name]

options:
  domain-source [session.logon.last.domain | none]
  headers [add | delete | modify | replace-all-with] {
    [name] {
      options:
        app-service [[string] | none]
        hname [[string] | none]
        hvalue [[integer] | none]
    }
  }
  ntlm-domain [[string] | none]
  password-source [session.sso.token.last.password | none]
  username-conversion [enabled | disabled]
  username-source [session.sso.token.last.username | none]

edit ntlmv1 [ [ [name] | [glob] | [regex] ] ... ]

options:
  all-properties
  non-default-properties

**Display**

list ntlmv1
list ntlmv1 [ [ [name] | [glob] | [regex] ] ... ]
show running-config ntlmv1
show running-config ntlmv1 [ [ [name] | [glob] | [regex] ] ... ]
options:
  all-properties
  non-default-properties
  one-line
  partition
show ntlmv1
show ntlmv1 [name]

Delete

  delete ntlmv1 [name]

Description

You can use this ntlmv1 component to configure a single sign-on NT LAN Manager, version 1 configuration object.

Examples

Creates an SSO ntlmv1 configuration object named myntlmv1:

  create ntlmv1 myntlmv1

Options

You can use these options with the ntlmv1 component:

  ◆ domain-source
     Specifies the Session variable used as a source for the single sign-on user domain. The default value is session.logon.last.domain.
  ◆ headers
     Specifies the name and value of the HTTP header content to be inserted in an HTTP Request that passes through the APM SSO module. The default value is none.
     
     The options are:
     
     • hname
        Specifies the name of the HTTP header.
     • hvalue
        Specifies the value of the HTTP header.
  ◆ name
     Specifies the name for the SSO ntlmv1 configuration object. This option is required.
  ◆ ntlm-domain
     Specifies the static domain setting. If the domain is not retrieved successfully from the source specified in the domain-source option, the system uses this value for the source.
◆ **password source**
   Specifies the source from which you want SSO to retrieve the password to use to authenticate applications. The default value is `session.sso.token.last.password`.

◆ **username-conversion**
   Enables or disables conversion of PREWIN2k/UPN user name input format to the format you want to use for SSO. The default value is `disabled`.

◆ **username-source**
   Specifies the source from which you want SSO to retrieve the user name used to authenticate applications.

**See also**

`sso basic`, `sso form-based`, `sso kerberos`, `sso ntlmv2`
ntlmv2

Configures a single sign-on (SSO) NT LAN Manager, version 2 (ntlmv2) configuration object.

Module

apm sso

Syntax

Configure the ntlmv2 component within the sso module using the syntax shown in the following sections.

Create/Modify

create ntlmv2 [name]
modify ntlmv2 [name]

options:
  domain-source [session.logon.last.domain | none]
  headers [add | delete | modify | replace-all-with] {
    [name] {
      options:
        app-service [[string] | none]
        hname [[string] | none]
        hvalue [[integer] | none]
    }
  }
  ntlm-domain [[string] | none]
  password-source [session.sso.token.last.password | none]
  username-conversion [enabled | disabled]
  username-source [session.sso.token.last.username | none]

edit ntlmv2 [ [ [name] | [glob] | [regex] ] ... ]

options:
  all-properties
  non-default-properties

Display

list ntlmv2
list ntlmv2 [ [ [name] | [glob] | [regex] ] ... ]
show running-config ntlmv2
show running-config ntlmv2 [ [ [name] | [glob] | [regex] ] ... ]
options:
  all-properties
  non-default-properties
  one-line
  partition
show ntlm2
show ntlm2 [name]

Delete

delete ntlm2 [name]

Description

You can use the ntlm2 component to configure a single sign-on NT LAN Manager, version 2 configuration object.

Examples

Creates an SSO ntlm2 configuration object named myntlmv2:
create ntlm2 myntlmv2

Options

You can use these options with the ntlm2 component:

♦ domain-source
  Specifies the Session variable used as a source for the single sign-on user domain. The default value is session.logon.last.domain.

♦ headers
  Specifies the name and value of the HTTP header content to be inserted in an HTTP Request that passes through the APM SSO module. The default value is none.
  The options are:
  • hname
    Specifies the name of the HTTP header.
  • hvalue
    Specifies the value of the HTTP header.

♦ name
  Specifies a name for the sso ntlm2 configuration object. This option is required.

♦ ntlm-domain
  Specifies the static domain setting. If the domain is not retrieved successfully from the source specified in the domain-source option, the system uses this value for the source.
◆ **password source**  
Specifies the source from which you want SSO to retrieve the password to use to authenticate applications. The default value is `session.sso.token.last.password`.

◆ **username-conversion**  
Enables or disables conversion of PREWIN2k/UPN user name input format to the format you want to use for SSO. The default value is `disabled`.

◆ **username-source**  
Specifies the source from which you want SSO to retrieve the user name used to authenticate applications.

See also

`sso basic, sso form-based, sso kerberos, sso ntlmv1`
asm Module Components

- Introducing the asm module
- Alphabetical list of components
Introducing the asm module

You can use the tmsh components that reside within the asm module to configure BIG-IP® Application Security Manager™. For more information about the tmsh hierarchical structure, see Chapter 2, Understanding and Using the Traffic Management Shell.

Alphabetical list of components

The remainder of this chapter lists the tmsh components that are available in the asm module.
device-sync

Contains the ASM™ timestamp for each device in the group.

Module

asm

Syntax

Retrieve the list of the device-sync values using the syntax shown in the following section.

Display

list device-sync
list device-sync [ [name] | [glob] | [regex] ] ...

Description

Use this command to display the current values of the device-sync object, that is, ASM change times for all devices in the group.

This object is designed for internal purposes only (incremented on every ASM change), so do not try to create, modify, or delete it manually.

Examples

Displays all last ASM change times of the device group:

list device-sync

See also

glob, list, regex, tmsh
**httpclass-asm**

Configures initial ASM settings for applications.

**Module**

`asm`

**Syntax**

Configure the `httpclass-asm` component within the `asm` module using the syntax shown in the following sections.

**Create/Modify**

```plaintext
create httpclass-asm [name]
modify httpclass-asm [name]
options:
  active-policy-name [string]
  language [language]
  predefined-policy [predefined-policy]
```

**Display**

```plaintext
list httpclass-asm
list httpclass-asm [ [ [name] | [glob] | [regex] ] ... ]
show running-config httpclass-asm
show running-config httpclass-asm [ [ [name] | [glob] | [regex] ] ... ]
options:
  all-properties
  non-default-properties
  partition
```

**Delete**

```plaintext
delete httpclass-asm [name]
```

**Description**

Use this command to create, modify, display, or delete an `httpclass-asm` profile that configures ASM security policies. Changing or setting attributes for an `httpclass-asm` profile affects the ASM security policy with the same name.
Note that modifying the language of an existing profile reconfigures the ASM security policy and deletes the configurations, log entries, and statistics of the security policy.
This is for advanced usage; this command is intended for use by the application templates system (iApps™).

Examples

Creates a custom **httpclass-asm** profile named **my_class** that causes ASM to configure a security policy that has the utf-8 application language and the Rapid Deployment security policy:

```bash
create asm httpclass-asm my_class active-policy-name my_class_policy language utf-8 predefined-policy POLICY_TEMPLATE_RAPID_DEPLOYMENT_HTTP
```

Displays the properties of all **httpclass-asm** profiles:

```bash
list httpclass-asm
```

Options

You can use these options with the **httpclass-asm** component:

- **active-policy-name**
  Specifies the name of the active security policy. This option is deprecated. The active security policy name is identical to the HTTP class profile's name.

- **language**
  Specifies the language of the web application that the ASM security policy is protecting. Use autocomplete or **list /asm webapp-language** to get the list of supported languages.

- **name**
  Specifies a unique name for the component. This option is required for the commands **create**, **delete**, and **modify**.

- **predefined-policy**
  Specifies a predefined security policy for a web application. This security policy was prebuilt to provide out-of-the-box security for a known application. Use autocomplete to get a list of applications for which ASM has predefined policies.

See also

predefined-policy

Lists the available predefined policies that can be used in the context of the httpclass-asm profile.

Module

asm

Syntax

Retrieve the list of the predefined-policy values using the syntax shown in the following sections.

Display

list predefined-policy
list predefined-policy [ [ [name] | [glob] | [regex] ] ... ]

options:

app-service

Description

Use this command to display the possible values of the predefined-policy object to be used in the context of the httpclass-asm profile.
This is for advanced usage; this command is intended for use by the application templates system (iApps ™).

Examples

Displays all the predefined policies supported by the ASM:

list predefined-policy

Options

You can use this option with the predefined-policy component:

- **app-service**
  Displays the application service to which the object belongs. The default value is none.

  **Note:** If the strict-updates option is enabled on the Application Service that owns the object, you cannot modify or delete the object. Only the Application Service can modify or delete the object.
See also

delete, edit, glob, list, ltm virtual, modify, regex, reset-stats, show, tmsh
webapp-language

Lists the available languages that can be used in the context of the httpclass-asm profile.

Module

asm

Syntax

Retrieve the list of the webapp-language values using the syntax shown in the following sections.

Display

list webapp-language
list webapp-language [ [ [name] | [glob] | [regex] ] ... ]
   options:
       app-service

Description

Use this command to display the possible values of the webapp-language object to be used in the context of the httpclass-asm profile.
This is for advanced usage - this command is intended to be used by the application templates system.

Examples

Displays all the languages supported by the ASM:

list webapp-language
Options

You can use this option with the `webapp-language` component:

- **app-service**
  Displays the application service to which the object belongs. The default value is `none`.

**Note**

If the `strict-updates` option is enabled on the Application Service that owns the object, you cannot modify or delete the object. Only the Application Service can modify or delete the object.

See also

create, delete, edit, glob, list, ltm virtual, modify, regex, reset-stats, show, tmsh
auth Module Components

- Introducing the auth module
- Alphabetical list of components
Introducing the auth module

You can use the tmsh components that reside within the auth module to configure user authentication. For more information about the tmsh hierarchical structure, see Chapter 2, Understanding and Using the Traffic Management Shell.

Alphabetical list of components

The remainder of this chapter lists the tmsh components that are available in the auth module.
cert-ldap

Configures an LDAP configuration object for implementing Single Sign On based on a valid client certificate for BIG-IP® system users. The user is required to properly configure the apache for client certificate validation.

Module

auth

Syntax

Configure the cert-ldap component within the auth module using the following syntax.

Create/Modify

```
create cert-ldap [name]
modify cert-ldap [name]
options:
  bind-dn [ [account dn] | none]
  bind-pw [ [password] | none]
  bind-timeout [integer]
  check-host-attr [disabled | enabled]
  check-roles-group [disabled | enabled]
  debug [disabled | enabled]
  description [string]
  filter [ [filter name] | none]
  idle-timeout [integer]
  ignore-auth-info-unavail [no | yes]
  ignore-unknown-user [disabled | enabled]
  login-attribute [ [account name] | none]
  login-filter [ [string] | none]
  login-name [ [ldap attribute] | none]
  port [ [name] | [integer] ]
  scope [base | one | sub]
  search-base-dn [ [search base dn] | none]
  search-timeout [integer]
  servers [add | delete | replace-all-with] { [ [ip address] | [server name] ...] }
servers none
  ssl [disabled | enabled]
  ssl-ca-cert-file [ [file name] | none]
  ssl-check-peer [disabled | enabled]
```
The CERT-LDAP authentication mode is required to provide Single Sign On capability to the control plane based on a valid client certificate. This mode involves configuring an Apache server to initiate a client certificate request, perform certificate validation against an OCSP server, and then authenticate/authorize certificate credentials against a configured remote LDAP server or a Microsoft® Windows® Active Directory®. The mode is not based on basic HTTP authentication (that is, user name and password). CERT-LDAP mode is equivalent to LDAP mode with custom attributes.

To authenticate BIG-IP system users when their authentication data is stored on a remote LDAP server, you create an LDAP configuration object, and then activate the object. Make sure that Apache is configured to support the client certificate validation.
To configure CERT-LDAP authentication for BIG-IP system users

1. Use the cert-ldap component in the auth module to configure an LDAP configuration object.

2. To activate LDAP authentication for BIG-IP system users, type the following command sequence:

   ```
   modify / auth source type cert-ldap
   ```

Examples

Creates a configuration object named `bigip_cert_ldap_auth`:

```
create cert-ldap bigip_cert_ldap_auth servers add {my_ldap_server}
```

Deletes the configuration object named `bigip_cert_ldap_auth`:

```
delete ldap bigip_cert_ldap_auth
```

Options

You can use these options with the cert-ldap component:

- **bind-dn**
  - Specifies the distinguished name of an account to which to bind to perform searches. This search account is a Read-only account. You can also use the admin account as the search account. If an administrative distinguished name is not specified, then a bind is not attempted. The default value is `none`.
  
  **Note:** If the remote server is a Microsoft Windows Active Directory server, the distinguished name must be in the form of an email address.

- **bind-pw**
  - Specifies the password for the search account created on the LDAP server. This option is required if you enter a value for the bind-dn option. The default value is `none`.

- **bind-timeout**
  - Specifies a bind timeout limit, in seconds. The default value is `30`.

- **check-host-attr**
  - Confirms the password for the bind distinguished name. This option is optional. The default value is `disabled`.

- **check-roles-group**
  - Specifies whether to verify a user's group membership given in the remote-role definitions, formatted as `*member*of="group-dn"`. The default value is `disabled`.

- **debug**
  - Enables or disables syslog-ng debugging information at the LOG DEBUG level. The default value is `disabled`. F5 Networks does not recommend using this option for normal configuration.
- **description**  
  User-defined description.

- **filter**  
  Specifies a filter. Use this option for authorizing client traffic. The default value is **none**.

- **glob**  
  Displays the items that match the **glob** expression. For a description of **glob** expression syntax, see the **glob** man page.

- **group-dn**  
  Specifies the group distinguished name. The system uses this option for authorizing client traffic. The default value is **none**.

- **group-member-attribute**  
  Specifies a group member attribute. The system uses this option for authorizing client traffic. The default value is **none**.

- **idle-timeout**  
  Specifies the idle timeout, in seconds, for connections. The default value is **3600** seconds.

- **ignore-auth-info-unavail**  
  Specifies whether the system ignores authentication information if it is not available. The default value is **no**.

- **ignore-unknown-user**  
  Specifies whether the system ignores a user that is unknown. The default value is **disabled**.

- **login-attribute**  
  Specifies a logon attribute. Normally, the value for this option is **uid**; however, if the server is a Microsoft Windows Active Directory server, the value must be the account name **samaccountname** (not case-sensitive). The default value is **none**.

- **login-filter**  
  Specifies the filter to be applied on the CN of the client certificate. This filter is a regular expression to extract required information from CN of client certificate which will be used to match against LDAP search results. The default is **disabled**.

- **login-name**  
  Specifies the LDAP attribute to be used as a login name. The default is **disabled**.

- **name**  
  Specifies a unique name for the component. This option is required for the **create** and **modify** commands.

- **partition**  
  Displays the administrative partition within which the component resides.

- **port**  
  Specifies the port number or name for the LDAP service. Port **389** is typically used for non-SSL and port **636** is used for an SSL-enabled LDAP service. The default value is **ldap**.
◆ **regex**
Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. For a description of regular expression syntax, see the `regex` man page.

◆ **scope**
Specifies the search scope. The default value is `sub`. The possible values are:

  • **base**
    The search scope is base object. The `base` value is almost never useful for name service lookups.

  • **one**
    The search scope is one level.

  • **sub**
    The search scope is a subtree.

◆ **search-base-dn**
Specifies the search base distinguished name. The default value is `none`.

◆ **search-timeout**
Specifies the search timeout, in seconds. The default value is `30` seconds.

◆ **servers**
Specifies the LDAP servers that the system must use to obtain authentication information. You must specify a server when you create an LDAP configuration object.

◆ **ssl**
Enables or disables SSL functionality. The default value is `disabled`.

*Note: When you use `tmsh` to enable SSL for an LDAP service, the system does not change the port number from 389 to 636, as is required. To change the port number from the command line, use the `port` option, for example: `ldap [name] ssl enabled port 636`.*

◆ **ssl-ca-cert-file**
Specifies the name of an SSL CA certificate using the full path to the file. The default value is `none`.

◆ **ssl-check-peer**
Specifies whether the system checks an SSL peer. The default value is `disabled`.

◆ **ssl-ciphers**
Specifies SSL ciphers. The default value is `none`.

◆ **ssl-client-cert**
Specifies the name of an SSL client certificate. The default value is `none`.

◆ **ssl-client-key**
Specifies the name of an SSL client key. The default value is `none`.

◆ **sso**
Enables or disables Single Sign On (SSO) functionality. SSO eliminates the need to administer and maintain multiple user logons and eliminates
the need for users to enter their credentials multiple times. When SSO is disabled, the user will be prompted to authenticate into the BIG-IP. The default is off.

◆ **user-template**
  Specifies a user template for the LDAP application to use for authentication. The default value is none.

◆ **version**
  Specifies the version number of the LDAP application. The default value is 3.

◆ **warnings**
  Enables or disables warning messages. The default value is enabled.

See also

auth user, create, delete, glob, list, modify, regex, run, show, tmsh
Chapter 15

**Idap**

Configures an LDAP configuration object for implementing remote LDAP-based authentication of BIG-IP® system users.

**Module**

`auth`

**Syntax**

Configure the **ldap** component within the **auth** module using the following syntax.

**Create/Modify**

```plaintext
create ldap [name]
modify ldap [name]

options:
  bind-dn  [ [account dn] | none]
  bind-pw   [ [password] | none]
  bind-timeout [integer]
  check-host-attr [disabled | enabled]
  debug [disabled | enabled]
  description [string]
  filter   [ [filter name] | none]
  group-dn [ [group dn] | none]
  group-member-attr [ [attribute] | none]
  idle-timeout [integer]
  ignore-auth-info-unavail [no | yes]
  ignore-unknown-user [disabled | enabled]
  login-attribute [ [account name] | none]
  port    [ [name] | [integer] ]
  scope   [base | one | sub]
  search-base-dn [ [search base dn] | none]
  search-timeout [integer]

servers [add  | delete  | replace-all-with]
  { [ [ip address] | [server name] ... ] }

servers none

ssl [disabled | enabled]

ssl-ca-cert-file  [ [file name] | none]
ssl-check-peer [disabled | enabled]

ssl-ciphers [ [string] | none]
ssl-client-cert [ [string] | none]
```
Description

LDAP authentication is useful when the BIG-IP system users authentication or authorization data is stored on a remote LDAP server or a Microsoft® Windows® Active Directory® server, and you want the user credentials to be based on basic HTTP authentication (that is, user name and password).

To authenticate BIG-IP system users when their authentication data is stored on a remote LDAP server, you create an LDAP configuration object, and then activate the object.

**To configure LDAP authentication for BIG-IP system users**

1. Use the ldap component in the auth module to configure an LDAP configuration object.
2. To activate LDAP authentication for BIG-IP system users, type the following command sequence:
   
   ```
   modify / system global-settings auth-source-type radius
   ```
Examples

Creates a configuration object named bigip_ldap_auth:
create ldap bigip_ldap_auth servers add {my_ldap_server}

Deletes the configuration object named bigip_ldap_auth:
delete ldap bigip_ldap_auth

Options

You can use these options with the ldap component:

◆ **bind-dn**
  Specifies the distinguished name of an account to which to bind to perform searches. This search account is a Read-only account. You can also use the admin account as the search account. If an administrative distinguished name is not specified, then a bind is not attempted. The default value is none.

  *Note: If the remote server is a Microsoft Windows Active Directory server, the distinguished name must be in the form of an email address.*

◆ **bind-pw**
  Specifies the password for the search account created on the LDAP server. This option is required if you enter a value for the bind-dn option. The default value is none.

◆ **bind-timeout**
  Specifies a bind timeout limit, in seconds. The default value is 30.

◆ **check-host-attr**
  Confirms the password for the bind distinguished name. This option is optional. The default value is disabled.

◆ **debug**
  Enables or disables syslog-ng debugging information at the LOG DEBUG level. The default value is disabled. F5 Networks does not recommend using this option for normal configuration.

◆ **description**
  User-defined description.

◆ **filter**
  Specifies a filter. Use this option for authorizing client traffic. The default value is none.

◆ **glob**
  Displays the items that match the glob expression. For a description of glob expression syntax, see the glob man page.

◆ **group-dn**
  Specifies the group distinguished name. The system uses this option for authorizing client traffic. The default value is none.

◆ **group-member-attribute**
  Specifies a group member attribute. The system uses this option for authorizing client traffic. The default value is none.
◆ **idle-timeout**
   Specifies the idle timeout, in seconds, for connections. The default value is **3600** seconds.

◆ **ignore-auth-info-unavail**
   Specifies whether the system ignores authentication information if it is not available. The default value is **no**.

◆ **ignore-unknown-user**
   Specifies whether the system ignores a user that is unknown. The default value is **disabled**.

◆ **login-attribute**
   Specifies a logon attribute. Normally, the value for this option is **uid**; however, if the server is a Microsoft Windows Active Directory server, the value must be the account name **samaccountname** (not case-sensitive). The default value is **none**.

◆ **name**
   Specifies a unique name for the component. This option is required for the **create** and **modify** commands.

◆ **partition**
   Displays the administrative partition within which the component resides.

◆ **port**
   Specifies the port number or name for the LDAP service. Port **389** is typically used for non-SSL and port **636** is used for an SSL-enabled LDAP service. The default value is **ldap**.

◆ **regex**
   Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. For a description of regular expression syntax, see the **regex** man page.

◆ **scope**
   Specifies the search scope. The default value is **sub**. The possible values are:
   - **base**
     The search scope is base object. The **base** value is almost never useful for name service lookups.
   - **one**
     The search scope is one level.
   - **sub**
     The search scope is a subtree.

◆ **search-base-dn**
   Specifies the search base distinguished name. The default value is **none**.

◆ **search-timeout**
   Specifies the search timeout, in seconds. The default value is **30** seconds.

◆ **servers**
   Specifies the LDAP servers that the system must use to obtain authentication information. You must specify a server when you create an LDAP configuration object.
◆ ssl
   Enables or disables SSL functionality. The default value is disabled.
   Note: When you use tmsh to enable SSL for an LDAP service, the system
does not change the port number from 389 to 636, as is required. To
change the port number from the command line, use the port option, for
example: ldap [name] ssl enabled port 636.
◆ ssl-ca-cert-file
   Specifies the name of an SSL CA certificate using the full path to the file.
The default value is none.
◆ ssl-check-peer
   Specifies whether the system checks an SSL peer. The default value is
disabled.
◆ ssl-ciphers
   Specifies SSL ciphers. The default value is none.
◆ ssl-client-cert
   Specifies the name of an SSL client certificate. The default value is none.
◆ ssl-client-key
   Specifies the name of an SSL client key. The default value is none.
◆ user-template
   Specifies a user template for the LDAP application to use for
authentication. The default value is none.
◆ version
   Specifies the version number of the LDAP application. The default value
is 3.
◆ warnings
   Enables or disables warning messages. The default value is enabled.

See also
auth user, create, delete, glob, list, modify, regex, run, show, tmsh
login-failures

Displays or resets the status of the accounts of users whose attempts to log in to the BIG-IP system have failed.

Module

auth

Syntax

Configure the login-failures component within the auth module using the following syntax.

Modify

reset-stats login-failures
  options:
    username

Display

show login-failures
  options:
    field-fmt
    username

Description

Users assigned the role of Administrator can reset the status of the account of a user who is locked out of the BIG-IP system due to enforcement of a company's security requirements. Users assigned other roles can only view login failures.

Examples

Displays the login failure status of all users:
show login-failures

Displays the login failure status of the user joe:
show login-failures joe

Resets the failed login counters for all users to zero and unlocks all users:
reset-stats login-failures
Resets the failed login counter for the user **joe** to zero and unlocks the user **joe**:

```
reset-stats login-failures joe
```

#### Options

You can use these options with the **login-failures** component:

- **show**
  
  For information about the options that you can use with the **show** command, see `help show`.

- **username**
  
  Specifies a user account to display or reset.

#### See also

- `auth user`, `reset-stats`, `show`, `tmsh`
auth Module Components

**partition**

Configures administrative partitions that implement access control for BIG-IP system users.

**Module**

auth

**Syntax**

Configure the partition component within the auth module using the following syntax.

**Create/Modify**

create partition [name]
modify partition [name]
    options:
       default-route-domain [route domain ID]
       description [string]

**Display**

list partition
list partition [ [ [name] | [glob] | [regex] ] ...]
show running-config partition
show running-config partition [ [ [name] | [glob] | [regex] ] ...]
    options:
       all-properties
       non-default-properties
       one-line

**Delete**

delete partition [name]
    options:
       all

**Description**

An administrative partition is a logical container that you create, containing a defined set of BIG-IP system objects, such as virtual servers, pools, and profiles. When a specific set of objects resides in a partition, you can then
give certain users the authority to view and manage the objects in that partition only, rather than all objects on the BIG-IP system. This gives a finer degree of administrative control.

◆ Tip

_You can configure administrative partitions, only if the Administrator user role is assigned to your user account._

Examples

Creates a partition named `partition_A` that contains objects related to `application_A`:

```bash
create partition partition_A description "Repository for application_A objects"
```

Deletes the partition named `partition_B`:

```bash
delete partition partition_B
```

Options

You can use these options with the `partition` component:

◆ **description**
  Describes the contents of the partition. If you use spaces in the description, you must put quotation marks around the descriptive text, for example: _“This partition contains local traffic management objects for managing HTTP traffic.”_

◆ **default-route-domain**
  Specifies the ID of the route domain that is associated with the IP addresses that reside in the partition. For more information, see _route-domain_, on page 35-30.

◆ **glob**
  Displays the items that match the `glob` expression. For a description of `glob` expression syntax, see the _glob_ man page.

◆ **name**
  Specifies a unique name for the component. This option is required for the `create` and `modify` commands.

◆ **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. For a description of regular expression syntax, see the _regex_ man page.

See also

`auth user`, `create`, `delete`, `list`, `modify`, `net route domain`, `regex`, `show`, `tmsh`
**password**

Prompts for modification of a password and for a confirmation of the new password.

**Module**

`auth`

**Syntax**

Configure the `password` component within the `auth` module using the following syntax.

**Modify**

`modify password`

**Description**

If you are assigned the user role of **Administrator** or **User Manager**, you can change another user’s password. For example, from within the `auth` module, type the following command sequence:

```
modify password [user name]
```

The system prompts you to change the password for the specified user, and then to confirm the new password.

If you are assigned any other user role, the system prompts you to change your own password, and then confirm your new password.

To change a password from within another module, use the full path to the password.

**Examples**

From within the `auth` module, displays the **new password**: prompt:

```
(tmos.auth)# modify password
```

From within the `gtm` module, displays the **new password**: prompt:

```
(tmos.gtm)# modify / auth password
```

**See also**

`auth user`, `modify`, `tmsh`
Chapter 15

password-policy

Specifies the parameters of the valid passwords for the BIG-IP system.

Module

auth

Syntax

Configure the password-policy component within the auth module using the syntax shown in the following sections.

Modify

modify password-policy [name]

options:
  expiration-warning [integer]
  max-duration [integer]
  max-login-failures [integer]
  min-duration [integer]
  minimum-length [integer]
  password-memory [integer]
  policy-enforcement [disabled | enabled]
  required-lowercase [integer]
  required-numeric [integer]
  required-special [integer]
  required-uppercase [integer]

Display

list password-policy
list password-policy [name]
show running-config password-policy
show running-config password-policy [name]

options:
  all-properties
  non-default-properties
  one-line
Description

Users assigned a role of Administrator or Resource Administrator can modify a password policy for the BIG-IP system to enforce a company's security requirements by defining the parameters for valid passwords. Users assigned other roles can view password policies.

Examples

Creates a password policy that specifies that passwords are valid for a maximum of 90 days and a minimum of 30 days. Also specifies that to be valid, a password must contain at least six characters, but not more than 10 characters, including two lowercase alpha characters, two uppercase alpha characters, and one number. Additionally, this policy specifies that the system automatically warns users five days before their passwords expire:

```
password policy max-duration 90 min-duration 30 minimum-length 6 required-lowercase 2 \ 
required-uppercase 2 required-special 1 required-numeric 1 expiration-warning 5
```

Displays the password policy:

```
list password-policy
```

Options

You can use these options with the password-policy component:

- **expiration-warning**
  Specifies the number of days before a password expires. Based on this value, the BIG-IP system automatically warns users when their password is about to expire. The default value is 7 days.

- **max-duration**
  Specifies the maximum number of days a password is valid. The default value is 99999.

- **max-login-failures**
  Specifies the number of consecutive unsuccessful login attempts that the system allows before locking out the user. The default value is 0 (zero-disabled).

- **min-duration**
  Specifies the minimum number of days a password is valid. The default value is 0 (zero).

- **minimum-length**
  Specifies the minimum number of characters in a valid password. The default value is 6.

- **password-memory**
  Specifies whether the user has configured the BIG-IP system to remember a password on a specific computer. The default value is 0 (zero).
◆ **policy-enforcement**  
Enables or disables the password policy on the BIG-IP system. The default value is **disabled**.

◆ **required-lowercase**  
Specifies the number of lowercase alpha characters that must be present in a password for the password to be valid. The default value is **0** (zero).

◆ **required-numeric**  
Specifies the number of numeric characters that must be present in a password for the password to be valid. The default value is **0**.

◆ **required-special**  
Specifies the number of special characters that must be present in a password for the password to be valid. The default value is **0** (zero).

◆ **required-uppercase**  
Specifies the number of uppercase alpha characters that must be present in a password for the password to be valid. The default value is **0**.

### See also

auth user, modify, tmsh
```
radius

Configures a RADIUS configuration object for implementing remote RADIUS-based authentication of BIG-IP system users.

Module

auth

Syntax

Configure the radius component within the auth module using the following syntax.

Create/Modify

create radius [name]
modify radius [name]
    options:
        accounting-bug [disabled | enabled]
        client-id [none | [string] ]
        debug [disabled | enabled]
        description [string]
        retries [integer]
        servers [default | none]
        servers [add | delete | replace-all-with] { [ [hostname] | [ip address] ] ... }
        servers [default | none]
edit radius [ [ [name] | [glob] | [regex] ] ... ]
    options:
        all-properties
        non-default-properties

Display

list radius
list radius [ [ [name] | [glob] | [regex] ] ... ]
show running-config radius
show running-config radius [ [ [name] | [glob] | [regex] ] ... ]
    options:
        all-properties
        non-default-properties
        one-line
        partition
```
Delete

delete radius [name]

Description

To authenticate BIG-IP system users when their authentication data is stored on a remote RADIUS server, you configure a RADIUS server, configure a RADIUS configuration object that references that RADIUS server, and then activate RADIUS authentication for the BIG-IP system. In this case, client credentials are based on basic HTTP authentication (that is, user name and password).

To configure RADIUS authentication for the BIG-IP system

1. Use the radius-server component in the auth module to configure a RADIUS server.
   For more information about creating RADIUS server objects, see radius-server, on page 15-24.
2. Use the radius component in the auth module to create a RADIUS configuration object that references the RADIUS server you created in Step 1.
3. To activate RADIUS authentication for BIG-IP system users, type the following command sequence:
   modify / system global-settings auth-source-type radius

Examples

Creates a RADIUS configuration object named bigip_radius_auth:
create radius bigip_radius_auth servers add {myradiusserver}

Deletes the RADIUS configuration object named bigip_radius_auth:
delete radius bigip_radius_auth

Options

You can use these options with the radius component:

- accounting-bug
  Enables or disables validation of the accounting response vector. This option is necessary only on older servers. The default value is disabled.

- client-id
  Sends a NAS-Identifier RADIUS attribute with string bar. If you do not specify a value for the client-id option, the system uses the pluggable authentication module (PAM) service type. You can disable this feature by specifying a blank client ID.
auth Module Components

◆ debug
Enables or disables syslog-ng debugging information at the LOG DEBUG level. F5 Networks does not recommend this option for normal use. The default value is disabled.

◆ description
User-defined description.

◆ glob
Displays the items that match the glob expression. For a description of glob expression syntax, see the glob man page.

◆ name
Specifies a unique name for the component. This option is required for the create and modify commands.

◆ partition
Displays the partition within which the component resides.

◆ regex
Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. For a description of regular expression syntax, see the regex man page.

◆ retries
Specifies the number of authentication retries that the BIG-IP Local Traffic Manager™ system allows before authentication fails. The default value is 3.

◆ servers
Specifies the host names or IP addresses of existing RADIUS servers that the BIG-IP system uses to obtain authentication data.

See also

auth radius-server, auth user, create, delete, glob, list, modify, regex, run, show, tmsh
radius-server

Confirms a RADIUS server for implementing remote RADIUS-based authentication of BIG-IP system users.

Module

auth

Syntax

Configure the radius-server component within the auth module using the following syntax.

Create/Modify

create radius-server [name]
modify radius-server [name]
options:
  description [string]
  port [ [name] | [number] ]
  secret [none | ["string"] ]
  server [ [hostname] | [ip address] | none ]
  timeout [integer]
edit radius-server [ [ [name] | [glob] | [regex ] ] ... ]
options:
  all-properties
  non-default-properties

Display

list radius-server
list radius-server [ [ [name] | [glob] | [regex ] ] ... ]
show running-config radius-server
show running-config radius-server [ [ [name] | [glob] | [regex ] ] ... ]
options:
  all-properties
  non-default-properties
  one-line
  partition

Delete

delete radius-server [name]
auth Module Components

Description

To authenticate BIG-IP system users when their authentication data is stored on a remote RADIUS server, you configure a RADIUS server, configure a RADIUS configuration object that references that RADIUS server, and then activate RADIUS authentication for the BIG-IP system. In this case, client credentials are based on basic HTTP authentication (that is, user name and password).

To configure RADIUS authentication for the BIG-IP system

1. Use the `radius-server` component in the `auth` module to configure a RADIUS server.

2. Use the `radius` component in the `auth` module to create a RADIUS configuration object that references the RADIUS server you created in Step 1.

   For more information about creating a RADIUS configuration object, see `radius`, on page 15-21.

3. To activate RADIUS authentication for BIG-IP system users, type the following command sequence:

   ```
   modify / system global-settings auth-source-type radius
   ```

Examples

Creates a RADIUS server component named `bigip_auth_radius_server`:

```]
create radius-server bigip_auth_radius_server secret "This is the secret." server 10.1.1.1
```]

Deletes the RADIUS server named `bigip_auth_radius_server`:

```]
delete bigip_auth_radius_server my_radius_server
```]

Options

You can use these options with the `radius-server` component:

- **description**
  User-defined description.

- **glob**
  Displays the items that match the `glob` expression. For a description of `glob` expression syntax, see the `glob` man page.

- **name**
  Specifies a unique name for the component. This option is required for the `create` and `modify` commands.

- **partition**
  Displays the partition within which the component resides.

- **port**
  Specifies the port for RADIUS authentication traffic. The default value is 1812.
◆ **regex**
   Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. For a description of regular expression syntax, see the `regex` man page.

◆ **secret**
   Specifies the secret key the system uses to encrypt and decrypt packets sent from or received by the server. This option is required.

◆ **server**
   Specifies the host name or IP address of the RADIUS server. This option is required.

◆ **timeout**
   Specifies the timeout value in seconds. The default value is 3.

See also

auth radius, auth user, create, delete, glob, list, modify, regex, run, show, tmsh
remote-role

Creates a file (/config/bigip/auth/remoteroles) that an LDAP, Active Directory, RADIUS, or TACACS+ server reads to determine the specific access rights to grant to groups of remotely-authenticated users.

Module

auth

Syntax

Configure the remote-role component within the auth module using the following syntax.

Modify

modify remote-role
  options:
    description [string]
    role-info [add | delete | modify | replace-all-with] {
      [group-name] {
        options:
          attribute [string]
          console [enabled | disabled]
          description [string]
          deny [enabled | disabled]
          line-order [integer]
          role [acceleration-policy-editor | admin | application-editor | auditor | \\ certificate-manager | guest | irule-manager | manager | operator | \\ resource-admin | user-manager | web-application-security-administrator | \\ web-application-security-editor]
          user-partition [all | Common | [name] ]
          user-partition [%string]
      }
    }
    role-info none

Display

  list remote-role
  show running-config remote-role
  options:
    all-properties
    one-line
    non-default-properties
Delete

You cannot delete the remote-role defaults, you can only modify the values of the options.

Description

You can use the `remote-role` component to grant access to a specific group of remotely-authenticated users without creating a local user account on the BIG-IP system for each user in the group.

Users assigned the role of **Administrator** or **Resource Administrator** can modify remote roles. Users assigned all other roles can view remote roles.

You can use the variable substitution feature to assign access rights for a group of remote users by specifying a text string variable that is preceded by a leading `%` character for the options `attribute`, `console`, and `role`. For example, when you define the remote role for the groups DC1 and DC2 shown in the following example, the BIG-IP system attempts to match the value of the `attribute` option, `F5-LTM-User-Info-1=DC1`, and then pulls the value of the `console`, `user-partition`, and `role` options from the other variables.

```
remote-role {
  role info {
    dc1 {
      attribute "F5-LTM-User-Info-1=DC1"
      console %F5-LTM-User-Console
      line-order 1
      role %F5-LTM-User-Role
      user-partition %F5-LTM-User-Partition
    }
    dc2 {
      attribute "F5-LTM-User-Info-1=DC2"
      line-order 2
    }
  }
}
```

Note that if a variable includes an incorrect value, the system does not authorize the user. Additionally, if you have not defined the variables, as with the group **DC2** above, the system authenticates the user with the following access rights:

- console = disabled
- role = none
- user-partition = none
Examples

Configures a remote role, named `my_managers`, for LDAP authentication by creating the 1000th line of the `/config/bigip/auth/remoterole` file, and granting the `Manager` role (100) in all partitions to the remote users assigned this role:

```bash
modify remote-role role-info add { my_managers { attribute "memberOF=cn=BIG-IPmanagerGroup,cn=users,dc=mydept,dc=mycompany,dc=com" \ console disabled line-order 1000 role 100 user-partition all } }
```

Configures a remote role, named `my_admins`, for LDAP authentication by creating the 2000th line of the `/config/bigip/auth/remoterole` file, and granting the `Administrator` role (0) in all partitions to the remote users assigned this role:

```bash
modify remote-role role-info add { my_admins { attribute "memberOF=cn=BIG-IPadministratorGroup,cn=users,dc=mydept,dc=mycompany,dc=com" \ console enabled line-order 2000 role 0 user-partition all } }
```

Configures a remote role, named `my_managers`, for RADIUS authentication by creating the 3000th line of the `/config/bigip/auth/remoterole` file, and granting the `Administrator` role (0) in all partitions to the remote users assigned this role:

```bash
modify remote-role role-info add { my_managers { attribute "manager_group=manager" \ console enable line-order 3000 user-partition all } }
```

Options

You can use these options with the `remote-role` component:

- **description**
  Specifies a user-defined description.

- **role-info**
  Configures the access rights for a specific group of remotely-authenticated users. You can configure the following information for a remote role:

  - **attribute**
    Specifies an attribute-value pair that an authentication server supplies to the BIG_IP system to match against entries in `/config/bigip/auth/remoterole`. The specified pair typically identifies users with access rights in common. This option is required. Alternatively, you can use the variable substitution feature and specify a text string variable that is preceded by a leading `%` character.

  - **console**
    Enables or disables console access for the specified group of remotely-authenticated users. The default value is `disabled`. When using variable substitution, as described in the `Description` section above, the variable for the `role` option must evaluate to one of these values: `tmsh` or `bpsh`. If it does not, the `console` option is `disabled`. 
- **deny**
  Enables or disables remote access for the specified group of remotely-authenticated users. The default value is **disabled**.

- **description**
  Specifies a user-defined description.

- **group-name**
  Specifies the name of the remote role that you are configuring. This option is required.

- **line-order**
  Specifies the number of the first populated line in the file, `/config/bigip/auth/remoterole`. This is a required field.

  The LDAP, Active Directory, RADIUS, and TACACS+ servers read this file line by line. The order of the information is important; therefore, F5 Networks recommends that you set the first line at line **1000**. This allows you, in the future, to insert lines before the first line. This option is required.

- **role**
  Specifies the role that you want to grant to the specified group of remotely-authenticated users. The default value is **no-access**. This option is required. The available roles are:
  - **admin**
  - **application-editor**
  - **certificate-manager**
  - **guest**
  - **manager**
  - **no-access**
  - **operator**
  - **resource-admin**
  - **user-manager**
  - **web-application-security-administrator**
  - **web-application-security-editor**

  When using variable substitution, as described in the *Description* section above, the variable for the **role** option must evaluate to one of these values: 0 (admin), 20 (resource admin), 40 (user manager), 100 (manager), 300 (application editor), 400 (operator), 500 (certificate manager) 700 (guest), 800 (web application security administrator), 810 (web application security editor), 900 (no-access).

- **user-partition**
  Specifies the user partition to which you are assigning access to the specified group of remotely-authenticated users. The default value is **Common**. This option is required.

  Alternatively, you can use the variable substitution feature, as described in the *Description* section above, and specify a text string variable that is preceded by a leading `%` character.
See also

auth remote-user, auth user, list, modify, show, tmsh
**remote-user**

Configures the default role, partition access, and console access for all remotely authenticated user accounts that have not been added as local user accounts on the BIG-IP system.

**Module**

`auth`

**Syntax**

Configure the `remote-user` component within the `auth` module using the following syntax.

**Modify**

```bash
modify remote-user
  options:
    default-partition [all | Common | [partition name] ]
    default-role [acceleration-policy-editor | admin | application-editor | auditor | \ guest | iRule-manager | manager | no-access | operator | resource-admin | \ user-manager | web-application-security-administrator | \ web-application-security-editor]
    description [string]
    remote-console-access [bpsh | disabled | tmsh]
```

**Display**

```bash
list remote-user
show running-config remote-user
  options:
    all-properties
    non-default-properties
    one-line
```

**Delete**

You cannot delete the `remote-user` defaults; you can only modify the values of the options.

**Description**

You can use the `remote-user` component to configure the default parameters for all the remote user accounts on the BIG-IP system as a group. To assign a different access level to a specific remote user, you must create
a local user account for that user on the BIG-IP system. For more information, see user, on page 15-40.

Users assigned the role of Administrator or Resource Administrator can modify the parameters of the remote-user component. Users assigned all other roles can view the parameters of the remote-user component.

Examples

For all remote users, sets the default partition access to partition Common, the default role to no-access, and the default remote console access to disabled.

modify remote-user default-partition Common default-role no-access remote-console-access disabled

For all remote users, sets the default partition access to all partitions, the default role to no-access, and the default remote console access to disabled.

modify remote-user default-partition all default-role no-access remote-console-access disabled

Options

You can use these options with the remote-user component:

- **default-partition**
  Specifies the default partition for all remote user accounts. The default value is all.
- **default-role**
  Specifies the default role for all remote user accounts. The default value is no-access.
- **description**
  Specifies a user-defined description.
- **remote-console-access**
  Specifies whether you are granting this user access to tmsh or disabling remote console access for this user. The default value is disabled.

See also

auth remote-role, auth user, list, modify, show, tmsh
Chapter 15

source

Configures the authorization source type for a BIG-IP system.

Module

auth

Syntax

Configure the source component within the auth module using the following syntax.

Modify

modify source
  options:
    type [active-directory | ldap | local | radius | tacacs | cert-ldap]

Display

list source
list source [option]
  options:
    all-properties
    non-default-properties
    one-line

Description

You can use the source component to set up the authorization source type for the BIG-IP system.

Examples

Sets up the authorization source type as tacacs:
modify auth source type tacacs

Displays the authorization source type:
list auth source type
Options

You can use these options with the `source` component:

- **type**
  Specifies the default user authorization source. The default value is `local`. When user accounts that access the system reside on a remote server, the value of the this option is the type of server that you are using for authentication, for example, `ldap`.

See also

- `list`, `modify`, `tmsh`
tacacs

Configures a TACACS+ configuration object for implementing remote authentication of BIG-IP system users based on TACACS+.

Module

auth

Syntax

Configure the `tacacs` component within the `auth` module using the following syntax.

Create/ Modify

```
create tacacs [name]
modify tacacs [name]
```

options:
- accounting [send-to-first-server | send-to-all-servers]
- authentication [use-first-server | use-all-servers]
- debug [disabled | enabled]
- description [string]
- encryption [disabled | enabled]
- protocol [none | [protocol] ]
- secret [ "[string]" ]
- servers [add | delete | replace-all-with] { [ [hostname] | [ip address] ] ... }
- service [ [name] | none]

```
edit tacacs [ [ [name] | [glob] | [regex] ] ... ]
edit tacacs [ [ [name] | [glob] | [regex] ] ... ]
```

options:
- all-properties
- non-default-properties

Display

```
list tacacs
list tacacs [ [ [name] | [glob] | [regex] ] ... ]
show running-config tacacs
show running-config tacacs [ [ [name] | [glob] | [regex] ] ... ]
```

options:
- all-properties
- non-default-properties
- one-line
- partition
Delete

delete tacacs [name]

Description

To authenticate BIG-IP system users when their authentication data is stored on a remote TACACS+ server, you create a TACACS+ configuration object, and then activate the object.

To configure TACACS+ authentication for BIG-IP system users

1. Use the `tacacs` component in the `auth` module to configure a TACACS+ configuration object.
2. To activate TACACS+ authentication for BIG-IP system users, type the following command sequence:
   ```
   modify / auth-source-type tacacs
   ```

Examples

Creates a TACACS+ configuration object named `bigip_tacacs_auth`:

```
create tacacs bigip_tacacs_auth servers add {my_tacacs_server}
```

Deletes the TACACS+ configuration object named `bigip_tacacs_auth`:

```
delete tacacs bigip_tacacs_auth
```

Options

You can use these options with the `tacacs` component:

- **accounting**
  If multiple TACACS+ servers are defined and pluggable authentication module (PAM) session accounting is enabled, sends accounting start and stop packets to the first available server or to all servers. The default value is `send-to-first-server`.
  Possible values are:
  - **send-to-all-servers**
    The system sends accounting start and stop packets to all servers.
  - **send-to-first-server**
    The system sends accounting start and stop packets to the first available server.
- **authentication**
  Specifies the process the system employs when sending authentication requests. The default value is `use-first-server`.

  Possible values are:
  - **use-all-servers**
    The system sends an authentication request to each server until authentication succeeds or until the system has sent a request to all servers in the list.
  - **use-first-server**
    The system sends authentication requests to only the first server in the list.
  - **description**
    Specifies a user-defined description.

- **debug**
  Enables `syslog-ng` debugging information at the LOG DEBUG level. F5 Networks does not recommend this option for normal use. The default value is `disabled`.

- **encryption**
  Enables or disables encryption of TACACS+ packets. F5 Networks recommends this option for normal use. The default value is `enabled`.

- **glob**
  Displays the items that match the `glob` expression. For a description of `glob` expression syntax, see the `glob` man page.

- **name**
  Specifies a unique name for the component. This option is required for the `create` and `modify` commands.

- **0**
  Displays the administrative partition within which the component resides.

- **protocol**
  Specifies the protocol associated with the value specified in the `service` option, which is a subset of the associated service being used for client authorization or system accounting.

- **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (`@[regular expression]`) to indicate that the identifier is a regular expression. For a description of regular expression syntax, see the `regex` man page.

- **secret**
  Sets the secret key used to encrypt and decrypt packets sent or received from the server. This option is required.

- **servers**
  Specifies the host name or IP address of the TACACS+ server. This option is required.
• service
  Specifies the name of the service that the user is requesting to be
  authenticated to use. Identifying the service enables the TACACS+
  server to behave differently for different types of authentication requests.
  This option is required.

See also

auth user, create, delete, edit, glob, list, modify, regex, run, show, tmsh
Chapter 15

**user**

Configures user accounts for the BIG-IP system.

**Module**

auth

**Syntax**

Modify the **user** component within the **auth** module using the following syntax.

**Create/Modify**

```plaintext
create user [name]
modify user [name]
```

**options:**

```plaintext
description [text...]
partition-access [all | Common | [name] ]
password [text]
prompt-for-password
role [acceleration-policy-editor | admin | application-editor | auditor | certificate-manager | guest | irule-manager | manager | no-access | operator | resource-admin | user-manager | web-application-security-administrator | web-application-security-editor]
shell [name]
```

**Display**

```plaintext
list user
```

```plaintext
list user [ [name] | [glob] | [regex] ] ...
```

```plaintext
show running-config user
```

```plaintext
show running-config user [ [name] | [glob] | [regex] ] ...
```

**options:**

```plaintext
all-properties
encrypted-password
non-default-properties
one-line
partition
```

**Delete**

```plaintext
delete user [name]
```
Description

You can create user accounts where the user names differ only by case-sensitivity (for example: david and DAVID).

Only users with the Administrator or Resource Administrator user role can save user accounts. Therefore, if you have a user role other than one of these, and you are creating or modifying user accounts, when you are done with your work, you must contact an Administrator or Resource Administrator to save the user accounts to the bigip_sys.conf file.

Additionally, only users with the Administrator, Resource Administrator, or User Manager user role can view all of the user accounts in all of the partitions to which the user has access. Therefore, if you have a user role other than one of these, you can only view your own user account.

Examples

Creates a new user named nwinters with a role of Guest in all partitions:

```
create user nwinters role guest partition-access all
```

Creates a new user named tknox with a role of operator and sets the user's log-in password:

```
create user tknox { role operator password aBcD007
```

Displays the properties of all user accounts:

```
list user
```

Options

You can use these options with the user component:

- **description**
  Describes the user account in free form text.

- **encrypted-password**
  Displays the encrypted password for the user account.

- **glob**
  Displays the items that match the glob expression. For a description of glob expression syntax, see the glob man page.

- **name**
  Specifies a unique name for the component. This option is required for the create and modify commands.

  **Note:** User account names are case-sensitive.

- **partition**
  Displays the name of the administrative partition within which the component resides.

- **partition-access**
  Specifies the administrative partition to which the user has access.
◆ **password**
Set the user password during creation or modification of a user account
without prompting or confirmation. May not be used with
prompt-for-password. Passwords are hidden in log and history files.

◆ **prompt-for-password**
Indicates that the BIG-IP system prompts the administrator or user
manager for a password and a password confirmation for the account
when the account is created or modified.

◆ **regex**
Displays the items that match the regular expression. The regular
expression must be preceded by an at sign (@[regular expression]) to
indicate that the identifier is a regular expression. For a description of
regular expression syntax, see the **regex** man page.

◆ **role**
Specifies the user role that you want to assign to the user account. Use
the value **no-access** to indicate that you do not want to assign a user role
to the user account.

◆ **shell**
Specifies the shell to which the user has access. Valid values are:

  • **bash**
    Provides an unrestricted system prompt. You can assign access to the
    **bash** shell only to users with the **Administrator** or
    **Resource-Administrator** role. However, F5 Networks recommends
    that you do not give **bash** shell access to users with the
    **Resource-Administrator** user role unless they use the **tcpdump,**
    **ssldump,** or **qkview** utilities, or if they manage certificate and key
    files using the console. Instead, F5 Networks recommends that you
give these users **tmsh** access.

  • **none**
    Specifies no shell access. The user must use the Configuration utility.

  • **tmsh**
    Provides access to the Traffic Management shell (**tmsh**).

**See also**

auth partition, auth password, create, delete, list, modify, show, tmsh
cli Module Components

- Introducing the cli module
- Alphabetical list of components
Introducing the cli module

You can use the tmsh components that reside within the cli module to configure administrative partitions, aliases, and the command line preferences. For more information about the tmsh hierarchical structure, see Chapter 2, Understanding and Using the Traffic Management Shell.

Alphabetical list of components

The remainder of this chapter lists the tmsh components that are available in the cli module.
admin-partitions

Sets the administrative partition for a BIG-IP® configuration file.

Module

cli

Syntax

Configure the admin-partitions component within the cli module using the following syntax.

Modify

admin-partitions
  options:
    update-partition [name]

Description

You can use the admin-partitions component set the administrative partition in which configuration will be loaded when a configuration file is being loaded.

This component is available only from a configuration file that is being loaded using the sys config component with the file option.

Examples

Sets the administrative partition in which configuration will be loaded. Configuration that follows this directive will be place in partition_A:

cli admin-partitions { update-partition partition_A }

Options

You can use this option to configure the admin-partitions component:

- update-partition
  Sets the administrative partition in which you can configure objects.

See also

load, sys config, tmsh
**global-settings**

Configures settings for **tmsh**.

**Module**

**cli**

**Syntax**

Configure the **global-settings** component within the **cli** module using the following syntax.

**Create/Modify**

```bash
edit global-settings
options:
  all-properties
  non-default-properties
modify global-settings
options:
  audit [disabled | enabled]
  description [string]
  idle-timeout [disabled | integer]
  scf-backup-number [integer]
  service [name | number]
```

**Display**

```bash
list global-settings
list global-settings [option]
  options:
    all-properties
    non-default-properties
    one-line
```

**Delete**

You cannot delete the default global settings.

**Description**

You can use the **global-settings** component to configure the audit setting for the **tmsh** utility.
Examples

Enables auditing for tmsh:

```
modify global-settings audit enable
```

Set the user idle timeout from tmsh to 15 minutes:

```
modify global-settings idle-timeout 15
```

Options

You can use these options with the alias component:

- **audit**
  Specifies the global audit level for the tmsh utility. The audited commands are stored in `/var/log/audit`. The default value is `enabled`. The audit levels are:
  - `disabled`
    tmsh does not log commands that users enter.
  - `enabled`
    tmsh and utility audit only commands that users enter. The system does not audit the commands that the load command runs.

- **description**
  User-defined description.

- **idle-timeout**
  If not `disabled`, log a user in tmsh interactive mode out automatically after a specified set of minutes. An administrator can change the timeout value at any time and the new policy will take place immediately.

- **scf-backup-number**
  Specifies the number of backup single configuration files that the system stores when you enter the following command sequence in tmsh:

```
load sys config file
```

When you run the command, the system saves the single configuration file. By default, the system saves two backup single configuration files. For example, if you set the `scf-backup-number` option to 3, after you run the command sequence `tmsh load sys config file` for the third time, the system has three versions of the single configuration file: `/var/local/scf/backup.scf`, `/var/local/scf/backup-1.scf`, and `/var/local/scf/backup-2.scf`. The newest file is `/var/local/scf/backup.scf`.

- **service**
  Specifies the format in which tmsh displays a service. The default value is `name`. The options are:
  - **name**
    Displays a service using a protocol name, for example, http.
  - **number**
    Displays a service using a numeric value, for example, 192.168.10.20:80, where 80 indicates http.
See also

edit, list, modify, run, show, tmsh
**history**

Displays a list of commands in the order in which you previously ran them.

**Module**

**cli**

**Syntax**

Use the `history` component within the **cli** module to display a numbered list of commands in the order the commands were issued.

**Display**

```
show history
!
!!
! [string]
```

**Description**

You can use the **history** component to display a list of the commands that you have run in **tmsh**. The commands display in the order in which you ran them, and each command is identified by an entry ID. The larger the entry ID of the command, the more recently you ran the command.

To rerun a command from the history list, type `q` to close the list and return to the **tmsh** prompt, and then type an exclamation point (!) followed by the entry ID of the command that you want to run.

**Examples**

Either of the two following commands displays the command history list:

```
! or
show history
```

Runs the fifth command in the command history list:

```
!5
```

Runs the previously issued command:

```
!!
```

Runs the last command that begins with `create`:

```
!create
```
See also

show, tmsh
preference

Configures tmsh preferences.

Module cli

Syntax

Configure the preference component within the cli module using the following syntax.

Modify

edit preference
modify preference [option]

options:
    alias-path [string list]
    confirm-edit [disabled | enabled]
    display-threshold [integer]
    editor [nano | vi]
    history-date-time [disabled | enabled]
    history-file-size [integer]
    history-size [integer]
    keymap [default | emacs | vi]
    list-all-properties [disabled | enabled]
    pager [disabled | enabled]
    prompt { [avc-count config-sync-status current-folder fully-qualified-host host mcp-load-status mcp-state multi-line status user] | none }
    show-aliases [disabled | enabled]
    stat-units [default | exa | gig | kil | meg | peta | raw | tera | yotta | zetta]
    table-indent-width [integer]
    tcl-syntax-highlighting [disabled | enabled]
    video [disabled | enabled]
    warn [bell | disabled | visual-bell]

edit preference

options:
    all-properties

Display

list preference
list preference [option]
show running-config preference
show running-config preference [option]
  options:
    all-properties
    one-line

Description

You can use the preference component to configure tmsh to meet your specific needs.

Examples

Configures tmsh to retrieve up to 500 objects before requiring a user response to the question, “Display all items? (y/n).”:

modify preference display-threshold 500

Configures the maximum number of commands that a user can view in the command history list to be 80:

modify preference history-size 80

Configures the maximum number of commands that tmsh saves in a user’s .tmsh_history file to be 1000 commands:

modify preference history-file-size 1000

Options

You can use the following options with the preference component.

◆ alias-path
  Specifies the search paths for aliases. Aliases could be in multiple locations; only ones on the search paths can be used.

◆ confirm-edit
  Specifies whether the edit command prompts for confirmation before saving changes. The default value is enabled.

The value of this option does not affect the behavior of the editor if the changes made in the editor result in a failed update. In this case, tmsh always prompts the user to either re-edit the file or discard the changes. The options are:

◆ enabled
  tmsh prompts a user to either submit (y), discard (n), or edit (e) the changes made to a component within the editor.

◆ disabled
  tmsh does not prompt the user, but instead, immediately submits the changes made in the editor.
- **display-threshold**
  Specifies the maximum number of objects that `tmsh` displays without requiring a user response to the question, “Display all items? (y/n).” You can specify from 0 (zero) through 4,294,967,265 objects. If you set this option to 0 (zero), `tmsh` displays an unlimited number of objects without requesting a response.

- **editor**
  Specifies the editor that the `edit` command invokes. Users assigned the user role of **Administrator** can select **nano** or **vi**. Users assigned other user roles must use **nano**.

- **history-date-time**
  Specifies whether `tmsh` displays in the command history the date and time that each command was issued. The default value is **disabled**. The command history file, `~/.tmsh-history-[user]`, always contains the date and time that a command was issued.

- **history-file-size**
  Specifies the maximum number of `tmsh` commands that the system saves in each user’s `.tmsh_history` file.
  If you set this option to 0 (zero), the system does not save `tmsh` commands in the file. The maximum value is 100,000.
  For performance reasons, the system does not truncate the file after the user enters a command. Instead, the system truncates the file after the user exits the `tmsh`.

- **history-size**
  Specifies the number of commands that a user can view or search in the command history list. The maximum number of commands is 100,000. The default value is 500.
  If you set this option to 0 (zero), the system does not add commands to the list of commands in memory; however, the system does write commands to the `.tmsh_history` file, unless the **history-file-size** option is set to 0 (zero).
  When you change the value of this option, the system renumbers the commands listed in memory; however, the commands remain in the same order.

- **keymap**
  Specifies the keyboard bindings that you want `tmsh` to use. The default value is **default**. The options are **default**, **emacs**, and **vi**.

- **list-all-properties**
  Specifies whether the system displays all of the properties of a component by default when you run the `list` command. The default value is **disabled**.

- **pager**
  Specifies whether the system sends the output of the `tmsh` commands `list` and `show` to `less`. The default value is **enabled**.
prompt
Specifies the information that you want to display in the tmsh prompt.
By default the prompt displays:
user_name@host_name(tmos-current_module)#
The options are:

- **avc-count**
  Displays the current SELinux Access Vector Cache in the tmsh prompt. The value displayed in the prompt indicates the number of times SELinux has denied access to a protected resource. The default is to not display this information.

- **config-sync-status**
  Displays global sync status in the tmsh prompt. The status displayed in the prompt indicates the rolled-up sync status of all the device groups the local device is a member of. The default is to display this information.

- **current-folder**
  Displays the current working folder in the tmsh prompt. The default value is to not display this information.

- **fully-qualified-host**
  Displays the fully qualified host name in the tmsh prompt. The default is to not display this information.

- **host**
  Displays the host name in the tmsh prompt. The default value is to display the host name in the prompt.

- **mcp-load-status**
  Displays the configuration file load status in the tmsh prompt. This information is also available in the Last Configuration Load Status of the show sys mcp command output. The default is to not display this information.

- **mcp-state**
  Displays the running phase of the mcpd service in the tmsh prompt. This information is also available in the Running Phase of the show sys mcp command output. The default is to not display this information.

- **multi-line**
  Displays the tmsh prompt on multiple lines, with information on the first line, and a pound sign (#) on the second line, for example:
  
  (Common:all) operator1@6400(tmos.cli)
  
  #
  
  The multi-line option is disabled by default.

- **none**
  Sets the tmsh prompt to display (tmos.current_module)#, where the system replaces current_module with the name of the module within which you are working.

- **status**
  Displays the system status in the tmsh prompt. The default value is to display system status in the prompt.
• **user**
  Displays the user name in the **tmsh** prompt. The default value is to display the user name in the prompt.

• **show-aliases**
  Specifies whether the system displays aliases in the results of the command completion and context-sensitive help features. The default value is enabled.

• **stat-units**
  Specifies the default unit in which the system displays statistics. The options are:
  • **default**
    Displays data in the simplest units. For example, if the value of the data is 1,200,001, the system displays 1.20M; however, if the value of the data is 1,200, the system displays 1.2K.
  • **exa**
    Display data in parts per quintillion.
  • **gig**
    Displays data in parts per billion.
  • **kil**
    Displays data in parts per thousand.
  • **meg**
    Displays data in parts per million.
  • **peta**
    Displays data in parts per quadrillion.
  • **raw**
    Displays raw data.
  • **tera**
    Displays data in parts per trillion.
  • **yotta**
    Displays data in parts per septillion.
  • **zetta**
    Displays data in parts per sextillion.

• **table-indent-width**
  Specifies the indent width when **tmsh** displays the child object tables in a show command. You can specify from 0 (zero) through 10. If you set this option to 0 (zero), **tmsh** displays child object tables without any indent.

• **tcl-syntax-highlighting**
  Specifies whether Tcl syntax highlighting will be enabled in the editor. This setting only applies if your editor preference is set to vi. The default value is disabled.

• **video**
  Enables or disables any video features used to highlight text. The default value is enabled.
◆ warn
  Specifies how the system warns you when you make an incorrect keystroke. The default value is bell. The options are:
  - bell
    Sounds a bell.
  - disabled
    Disables the warning function.
  - visual-bell
    Displays a visual warning.

See also

edit, list, modify, show, tmsh
Automates `tmsh` Tool Command Language (Tcl).

### Module

`cli`

### Syntax

Configure the `script` component within the `cli` module using the following syntax.

**Edit**

- `create script [name]`
- `modify script [name]`
- `edit script [ { [name] | [glob] | [regex] } ... ]`
  
  **options:**
  
  - `all-properties`

**Display**

- `list script`
- `list script [ { [name] | [glob] | [regex] } ... ]`
- `show running-config script`
- `show running-config script [ { [name] | [glob] | [regex] } ... ]`
  
  **options:**
  
  - `all-properties`

**Delete**

- `delete script [name]`

**Run**

- `run script [name] [options ...]`
  
  **options:**
  
  - `file [file name] [options ...]`
  - `verbatim-arguments [file option] [file name] [options ...]`

The options that are available depend on which script you are running. The `file` option is limited to users with the role of `administrator`. 
Description

You can use the script component to build Tcl scripts to automate management of the BIG-IP system. By combining command aliases with scripts, you can extend tmsh to build commands that are customized to your environment.

To do this, place the content of the script inside one or more Tcl procedures. The contents of a script cannot exceed 65,000 bytes. However, a script can include other scripts. For more information about including scripts in other scripts, see page 16-21.

You can use the following procedures in the manner specified:

- **script::run**
  
  tmsh invokes the procedure script::run when you issue the command sequence run / cli script [name]. A script is run relative to the module in which the run command is invoked.

  The script::run procedure must be defined in the script named by the run command. Scripts that are included by tmsh::include are not required to implement the procedure script::run.

- **script::help**
  
  Provides context-sensitive help. A script is not required to implement script::help.

- **script::tabc**
  
  Provides context-sensitive help. A script is not required to implement script::tabc.

- **script::init**
  
  tmsh calls the procedure script::init before calling one of the following procedures: script::run, script::help, or script::tabc. The script::init procedure can use the Tcl variable tmsh::csh to determine which one of these three procedures tmsh invokes after tmsh:init.

  Additionally, you can use the procedure script::init to initialize global variables. A script is not required to implement script::init.

Examples

Creates or modifies the script myscript:

```
edit script myscript
```

Creates or modifies the scripts myscript and yoursclipt:

```
edit script myscript yoursclipt
```

Displays the contents of the script myscript:

```
list script myscript
```

Deletes the script myscript from the system:

```
delete script myscript
```
Runs the script `myscript`:

```
run script myscript [arguments ...]
```

The system passes arguments to the script in the following Tcl variables:

- `tmsh::argc`
  Contains the number of arguments including the name of the script.

- `tmsh::argv`
  Contains the list of argument values. The first item in `tmsh::argv` is always the name of the script.

**Tip**

You can create an alias for the command sequence `run / cli script [name]` using the `cli alias` component.

Runs the same commands as `run script myscript [arguments...]` above, except the system passes all arguments specified in the command as one argument to the script. Note that you do not need to enclose the argument list in double quotes, and you do not need to escape special characters:

```
run script verbatim-arguments myscript [arguments ...]
```

**Options**

You can use these options with the `script` component:

- **file**
  Specifies that the script to be run should come from a file located on the file system rather than a script from the configuration.

- **glob**
  Displays the items that match the `glob` expression. For a description of `glob` expression syntax, see the `glob` man page.

- **name**
  Specifies a name for the script. This option is required for the `edit` and `delete` commands.

- **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. For a description of regular expression syntax, see the `regex` man page.

- **verbatim-arguments**
  Specifies that the arguments at the end of the command should not be tokenized by `tmsh` prior to being sent to the script. This is useful when the script is wrapping another utility that takes arguments.
Configuration and status assessors

The following Tcl commands mirror `tmsh` commands. For example, the Tcl command `tmsh::create` accepts the same components, object identifiers, and properties that the `tmsh create` command accepts.

- `tmsh::cd [args...]`
  Runs the `cd` command using the specified arguments.
- `tmsh::cp [args...]`
  Runs the `cp` command using the specified arguments.
- `tmsh::create [args...]`
  Runs the `create` command using the specified arguments.
- `tmsh::delete [args...]`
  Runs the `delete` command using the specified arguments.
- `tmsh::install [args...]`
  Runs the `install` command using the specified arguments.
- `tmsh::generate [args...]`
  Runs the `generate` command using the specified arguments.
- `tmsh::list [args...]`
  Runs the `list` command using the specified arguments. The system returns the results as a string.
- `tmsh::load [args...]`
  Runs the `load` command using the specified arguments.
- `tmsh::modify [args...]`
  Runs the `modify` command using the specified arguments.
- `tmsh::publish [args...]`
  Runs the `publish` command using the specified arguments.
- `tmsh::pwd`
  Runs the `pwd` command.
- `tmsh::reset-stats [args...]`
  Runs the `reset-stats` command using the specified arguments.
- `tmsh::run [args...]`
  Runs the `run` command using the specified arguments.
- `tmsh::save [args...]`
  Runs the `save` command using the specified arguments.
- `tmsh::show [args...]`
  Runs the `show` command using the specified arguments. The system returns the results as a string.

The following Tcl commands provide structured access for retrieving configuration, statistics, and status information.

- `tmsh::get_config [args...]`
  Returns a list of Tcl objects. Each of these objects can be passed to the following commands that accept an `$obj` argument. The arguments for this command are the same as for the `tmsh list` command.
◆ tmsh::get_status [component] [args...]
Returns a list of Tcl objects that can be passed to the following commands that accept an $obj argument. The arguments for this command are the same as for the tmsh show command.

This command can only be used on components that accept the field-fmt option. The field-fmt option is automatically appended to the argument list. The tmsh help pages identify if a component supports the field-fmt option.

There are very few components that have status and statistics that do not support the field-fmt option, and in those cases you can use the Tcl command tmsh::show to retrieve the object in the form of a Tcl string object.

A component must be specified, for example: tmsh::get_status ltm pool

◆ tmsh::get_type $obj
Returns the type identifier associated with the object. The $obj argument must be an object that was returned by either of the Tcl commands tmsh::get_config or tmsh::get_status.

◆ tmsh::get_name $obj
Returns the object identifier associated with the object. The $obj argument must be an object that was returned by either of the Tcl commands tmsh::get_config or tmsh::get_status.

◆ tmsh::get_field_names [value | nested] $obj
Returns a list of field names (not the value associated with a field) that are present in an object. The value fields are simple values or lists (for example, an integer or a string). The nested fields are a collection of zero or more nested objects, where the nested objects have their own fields (for example, pool members and virtual server profiles).

The $obj argument must be an object that was returned by the Tcl commands tmsh::get_config or tmsh::get_status. If the object was retrieved using the Tcl tmsh::get_config command, the field names are identical to those that are displayed by the tmsh list command. If the object was retrieved using the Tcl tmsh::get_status command, the fields are identical to those that the system displays using the tmsh show command with the field-fmt option.

◆ tmsh::get_field_value $obj [field name] [Tcl variable]
Retrieves the value of field name. The Tcl variable is optional. The behavior of this command depends on whether field name is present in $obj and a Tcl variable is present in the command.

- If field name is present in $obj, and a Tcl variable is present, the Tcl variable is set to the value of field name and the command returns 1.
- If field name is not present in $obj, and a Tcl variable is present, the command returns 0 (zero).
- If field name is present in $obj, and a Tcl variable is not present, the command returns the field value.
If field name is not present in $obj, and a Tcl variable is not present, the command raises an error that causes the script to stop. You can use the Tcl command catch to recognize the error and continue to run the script.

The $obj argument must be an object that was returned by the Tcl tmsh::get_config or tmsh::get_status commands, or a nested object obtained from the Tcl tmsh::get_field_value command.

If the field is a set of nested objects, the Tcl object that the system returns is a list of objects, where each of the objects can contain fields.

Each of the objects can be passed to the Tcl tmsh::get_field_value command. If the field is not a nested object, the system returns a single Tcl string object.

Transaction control

The following Tcl commands are specific to the tmsh Tcl API. There are no corresponding commands available in tmsh.

- **tmsh::begin_transaction**
  Begins an update transaction. The Tcl tmsh::create, tmsh::delete, and tmsh::modify commands that are issued before the next Tcl tmsh::commit_transaction command are submitted as a single update. The system rolls back all of the commands if any of the commands fail.

- **tmsh::commit_transaction**
  Runs the commands that have been issued since the last Tcl tmsh::begin_transaction command. The system validates all of the commands against the running configuration. If any one of the commands fail, the system does not apply any of the commands to the running configuration.

- **tmsh::cancel_transaction**
  Cancels all commands that you have issued since the last Tcl tmsh::begin_transaction command.

*Important:* You cannot use these Tcl commands inside an active transaction:

- tmsh::list
- tmsh::show
- tmsh::get_config
- tmsh::get_status
Logging

You can use the following Tcl commands to generate log events. These commands affect the behavior of the script and do not affect `tmsh`. These commands are available only to users who have been assigned either the Administrator or Resource Administrator role.

- `tmsh::log_dest [screen | file]`
  Specifies whether the system sends events to the screen or to log files. If `file` is selected, log messages will be directed to `/var/log/ltm`.

- `tmsh::log_level [level]`
  Specifies the default severity level. The system does not log events below the specified level.
  
  The options, listed in decreasing order of severity, are:
  
  - `emerg`
  - `alert`
  - `crit`
  - `err`
  - `warning`
  - `notice`
  - `info`
  - `debug`

- `tmsh::log [level] "message..."`
  Logs the specified message. The level parameter is optional. The level can be one of those described in the Tcl `tmsh::log_level` command.

Custom iStats

Custom `counter`, `gauge`, and `string` fields can be created, modified, and retrieved using iRules® or `tmsh` scripts. These custom fields are created on first write and do not need to be declared separately.

Each custom field has a "key" that can be associated with a `tmsh` configuration object. This key is composed of a `tmsh` component dotted path, a specific object name or ID, the field type, and the field name. The entire key must be enclosed in quotes.

For example, "ltm.pool /Common/my_pool counter num_hits" refers to the `num_hits` counter associated with the LTM® pool named `my_pool`, located in the `Common` folder.

These custom fields are displayed with the `tmsh show` command on the associated object.

- `istats::incr [key] [amount]`
  Increments a custom counter by `amount`. 
- `istats::set [key] [value]`
  Sets a custom gauge or string to `value`. Setting a counter to an exact value will only set it in the local segment, but `istats::get` will always read the aggregated (not local) value.

- `istats::get [key]`
  Returns the latest aggregated value of the custom field or 0 (zero) if it does not exist ("" for string fields).

**Utilities**

The following commands are Tcl utility commands.

- `tmsh::clear_screen`
  Clears the screen and places the cursor at the upper left of the screen.

- `tmsh::display [variable | command output]`
  Provides access to the `tmsh` pager. Output generated with the Tcl command `puts` is not paged.

- `tmsh::display_threshold [integer]`
  When a script is run, the system disables the option cli preference display-threshold. This does not affect the .tmshrc file.
  You can use the Tcl command `tmsh::display_threshold` to re-enable the threshold. Re-enabling the threshold in this way causes the script to generate a prompt if you issue the commands `tmsh::list, tmsh::show, tmsh::get_config, or tmsh::get_status`, and the output that is generated exceeds the threshold. See help cli preference, for a description of this option and valid ranges for its value.

- `tmsh::include [script name]`
  Runs the Tcl command `eval` on the specified script. The system evaluates the script at a global level, and all procedures in the included script are available to any other procedure. You must have previously created the script that is being included using the `tmsh edit / cli script [name]` command. If a full path is not given for the script name, `tmsh` will attempt to first locate the script from the same folder as the including script, then the root partition folder of the including script, and finally the /Common folder.

- `tmsh::run_proc [script_name:proc_name] options...]`
  Runs the Tcl `eval` command on the specified script and process. The script `script_name` is loaded as if `tmsh::include` was called. After the script is loaded, the Tcl `eval` command is run on the specified Tcl process. Any options that were specified are passed to the Tcl process. This is essentially a short form of running `tmsh::include script_name`, followed by running one of the Tcl processes contained in the script that was included.
  
  The following example invokes the display_pool_status proc that is contained in the pool_utils script:

  `tmsh::run_proc pool_utils:display_pool_status`

- `tmsh::stateless [disabled | enabled]`
  Modifies the behavior of `tmsh::create` and `tmsh::delete`. 
When stateless mode is disabled, an attempt to create an object that already exists in the configuration results in an error, and an attempt to delete an object that does not exist in the configuration is in an error.

When stateless mode is enabled, an attempt to create an object that already exists in the configuration does not result in an error, and an attempt to delete an object that does not exist in the configuration does not result in an error.

Enabling stateless mode allows scripts to successfully run multiple times with the same input. The default value is disabled.

◆ tmsh::version
  Returns the version number of the BIG-IP system as a Tcl string. The version consists of three digits, a major, minor and maintenance version, separate by periods. For example, 10.1.0 indicates minor version 1 of major version 10.

Context-sensitive help

Use the following commands to create a script that provides context-sensitive help when a user types Tab or question mark (?).

◆ script::help
  Scripts can provide the script::help procedure. tmsh invokes the procedure when a user enters a question mark (?) while entering the command sequence run / cli script [name]. If the specified script includes the procedure script::init, tmsh invokes it before the procedure script::help. The script can add context-sensitive help by calling the procedures tmsh::add_help and tmsh::builtin_help. tmsh formats the help and displays it.

◆ script::tabc
  Scripts can provide the procedure script::tabc. The system invokes this procedure when the user types Tab while entering the command sequence run / cli script. If the procedure script::init is included in the script, that procedure is invoked before the procedure script::tabc. The script can add command completion datasets to the script by calling the procedures tmsh::add_tabc and tmsh::builtin_tabc. tmsh either formats and displays the command completion datasets, or, if possible, completes the current argument.

◆ tmsh::csh
  tmsh::csh is a Tcl string variable that can be used in the procedure script::init to determine the context in which the procedure script::init was invoked.

  tmsh::csh is set to one of the following:
  • question mark (?)
    Indicates that the user typed a question mark (?).
  • TABC
    Indicates the user pressed the Tab key.
  • an empty string ("")
    Indicates the script is being run.
cli Module Components

◆ **tmsh::add_help** [ [category item description] | [description] ]
  Displays context-sensitive help when the user types a questions mark (?).
  If you supply one argument, that argument displays as-is with no
  formatting applied to the description.
  If you supply three arguments, one or more datasets are constructed. The
  first argument is the name of the dataset. The second argument is an item
  in the dataset. The third argument is a description of the item. This
  command has an affect only if the Tcl variable $tmsh::csh is set to
  question mark (?).

◆ **tmsh::builtin_help** ["tmsh command" args...]
  Presents the same results as typing a question mark (?) while entering a
  tmsh command. The system stores a set of possible completions and
  displays the possibilities when the procedure script::help returns. This
  command has an effect only if the Tcl variable tmsh::csh is set to
  question mark (?).

◆ **tmsh::add_tabc** [ [category item] | [item] ]
  Adds completion datasets. If you supply one argument, the system adds
  that argument to an anonymous dataset. If you supply two arguments, the
  system constructs one or more datasets. The first argument is the name of
  the dataset. The second argument is an item in the dataset. Potential
  completions are displayed in groups based on category. This command
  has an affect only if the Tcl variable $tmsh::csh is set to TABC.

◆ **tmsh::builtin_tabc** ["tmsh command" args...]
  Many of the tmsh commands that are available for scripting are also
  available in the interactive shell. A script can use the tmsh::builtin_tabc
  command to present the same command completion results as a built-in
  command. The command does not return a value. The set of possible
  completions are stored internally and displayed when the procedure
  script::tabc returns. This command has an effect only if called during
  the Tcl variable $tmsh::csh is set to TABC.

Third party Tcl library usage

A selection of third party libraries have been tested to work within the CLI
script environment, including MD5, BASE64, SHA1/SHA256, HTTP, TLS,
TCL Perl, LDAP client, and XML parser. The TCL packages can only
reside in the directory of /usr/share/tcl8.4.

◆ **Important**

Only these tested packages are supported currently.
This example demonstrates the use of a Tcl package command to make use of tls/https. The TLS package is installed in the directory 
/usr/share/tcl8.4/tls in the form of two files: tls.tcl and libtls1.6.1.so.

```tcl
Modify script /Common/use_tls {
    proc script::run {} {
        set pkg_name tls
        set pkg_version 1.6
        package require http
        if {{catch (package require $pkg_name pkg_version)}} {
            puts "No package found: $pkg_name!\n"
        } else {
            puts "Found package: $pkg_name!\n"
            http::register https 443 tls::socket
            set token [http::geturl https://172.27.42.161/]
            upvar #0 $token state
            puts $state(http)
            puts $state(body)
        }
    }
}
```

This example uses the callback function to handle http data.

```tcl
cli script /Common/use_http2 {
    proc script::httpCallback {token} {
        upvar #0 $token state
        puts $state(http)
        puts $state(body)
        incr ::got_something
    }
    proc script::run {} {
        namespace eval :: {
            set got_something 0
        }
        set pkg_name http
        set pkg_version 2.4.5
        if {{catch (package require $pkg_name $pkg_version)}} {
            puts "No package found: $pkg_name!\n"
        } else {
            puts "Found package: $pkg_name!\n"
            http::geturl http://172.27.42.22/index.htm -command
            script::httpCallback
            vwait ::got_something
        }
    }
}
```
This example uses the LDAP client package to query data.

```tcl
cli script /Common/use_ldap {
    proc script::run {} {
        set pkg_name ldap
        if {{[catch {package require $ pkg_name 1.8}]} } {
            puts "No package found: $pkg_name!\n"
        } else {
            puts "Found package: $pkg_name!\n"
            set handle [ldap::connect 172.27.1.2]
            ldap::bind $handle
            set results [ldap::search $handle "dc=f5,dc=com" "(uid=test)" {}]
            foreach result $results {
                puts $result
            }
            ldap::unbind $handle
            ldap::disconnect $handle
        }
    }
}
```

Here are some additional examples:

```tcl
cli script /Common/use_parray {
    proc script::run {} {
        puts [info patch]
        namespace eval :: {
            set pkg_location /usr/share/tcl8.4/
            source [file join $pkg_location package.tcl]
        }
        puts "NS: [namespace current]"
        set pkg_location ::pkg_location
        source [file join $pkg_location parray.tcl]
        parray ::tcl_platform
    }
}
```

```tcl
cli script /Common/use_sha2 {
    proc script::run {} {
        set pkg_name sha256
        if {{[catch {package require $ pkg_name}]} } {
            puts "No package found: $pkg_name!\n"
        } else {
            puts "Found package: $pkg_name!\n"
            puts "TCL does SHA2 now!"
            puts [sha2::sha256 "TCL does SHA2"]
        }
    }
}
```
cli script /Common/use_tclperl {
proc script::run {} {
    set pkg_name tclperl
    if {[catch {package require $pkg_name}]} {
        puts "No package found: $pkg_name!\n"
    } else {
        puts "Found package: $pkg_name!\n"
        set interpreter [perl::interp new]
        $interpreter eval {print "Hello World\n"}
        perl::interp delete $interpreter
    }
}
}

Special characters

There are several characters that are part of both Tcl and tmsh syntax. You must escape these characters in a shell script so that Tcl passes them to tmsh. You can use standard Tcl escape characters, such as quotes and back slashes. You must escape curly braces ({}), for example: "{" "}".

Creates a Local Traffic Manager pool named my_pool.

tmsh::create ltm pool my_pool members add "{ 10.1.2.3:80 }"

Disabled commands

The following commands are disabled for users who have not been assigned a user role of Administrator or Resource Administrator:

- auto_execok
- auto_import
- auto_load
- auto_mkindex
- auto_mkindex_old
- auto_qualify
- auto_reset
- bgerror
- cd
- close
- eof
cli Module Components

- exec
- fblocked
- fconfigure
- fcopy
- file
- filevent
- filename
- flush
- glob
- http
- interp
- load
- memory
- open
- package
- pid
- pkg:create
- pkg_mkindex
- pwd
- seek
- socket
- source
- tcl_findLibrary
- tell
- unknown
- updates
- vwait

Examples

The following example demonstrates the use of all tmsh Tcl commands tmsh::obj<...>. The script displays all configuration property values or all status and statistic values for the specified component, depending on the specified arguments. The system displays all configuration settings if you replace [tmsh::get_config $comp all-properties] with [tmsh::get_config / all-properties]. The use of the all-properties option ensures that all options are displayed.

The following command sequence is an example of how to run the following script: run / cli script example.tcl config ltm pool

cli script example.tcl {
    proc script::init {} {

```
set ::field_fmt "%-25s %s"
set ::usage_string "usage: [lindex $tmsh::argv 0] \n    <config | status> <component path... name>"
}
proc script::help {} {
    if { $tmsh::argc < 2 } {
        tmsh::add_help Options: config "Display configuration"
        tmsh::add_help Options: status "Display status and statistics"
    } else {
        build_csh tmsh::builtin_help
    }
}
proc script::tabc {} {
    if { $tmsh::argc < 2 } {
        tmsh::add_tabc config
        tmsh::add_tabc status
    } else {
        build_csh tmsh::builtin_tabc
    }
}
proc script::run {} {
    if { $tmsh::argc < 3 } { usage } set opt [lindex $tmsh::argv 1] if { $opt != "config" && $opt != "status" } { usage }
    set comp ""
    for {set idx 2} {$idx < $tmsh::argc} {incr idx} {
        append comp [lindex $tmsh::argv $idx] "
    }
    if { $opt == "config" } {
        set objs [tmsh::get_config $comp all-properties]
    } else {
        set objs [tmsh::get_status $comp]
    }
    set idx 0
    set total [llength $objs]
    while { $idx < $total } {
        set obj [lindex $objs $idx]
print_object obj
puts ""
incr idx;
}
}
proc print_fields { objVar } {
upvar $objVar obj
set fdx 0
set fields [tmsh::get_field_names value $obj]
set field_count [llength $fields]
while { $fdx < $field_count } {
    set field [lindex $fields $fdx]
    puts [format $::field_fmt $field [tmsh::get_field_value $obj $field]]
    incr fdx
}
}
proc print_object { objVar } {
upvar $objVar obj
puts "[tmsh::get_type $obj] [tmsh::get_name $obj]"
# name/value pairs
print_fields obj

# nested objects
set fdx 0
set fields [tmsh::get_field_names nested $obj]
set count [llength $fields]
while { $fdx < $count } {
    set field [lindex $fields $fdx]
    set nested_objects [tmsh::get_field_value $obj $field]
    set ndx 0
    set n_count [llength $nested_objects]
    while { $ndx < $n_count } {
        set nobj [lindex $nested_objects $ndx]
        print_object nobj
        incr ndx
    }
    if {($n_count == 0) } {
        puts [format $::field_fmt $field "none"]
    }
    incr fdx
}
}
proc build_csh { command } {
# generate context-sensitive help, tab completion or "?"
set args ""
for {set idx 2} {$idx < $tmsh::argc} {incr idx} {
    lappend args [lindex $tmsh::argv $idx]
}
set opt [lindex $tmsh::argv 1]
if { $opt == "config" } {
    $command list $args
}
elseif { $opt == "status" } {
    $command show $args
}
else {
    puts "\nunexpected argument: $opt"
}
return $args
}
proc usage ( ) {
    puts $::usage_string
    exit
}

See also
cli alias, create, delete, edit, glob, list, modify, regex, reset-stats, show, tmsh
For information about Tcl, see www.tcl.tk.
transaction

Opens batch mode, where you can submit a set of commands as a single transaction.

Module

cli

Syntax

Use the transaction component within the cli module to open batch mode, enter a series of commands, and then submit the commands as a single transaction.

Create/Modify

create transaction
modify transaction
  options:
    delete [entry_id]
submit transaction

Display

list transaction

Delete

delete transaction

Description

tmsh parses each command that you enter in batch mode. If the command passes a syntax check, tmsh saves it as part of the transaction you are creating and returns a confirmation. After you finish adding commands, you submit the transaction to change the running configuration of the system. The system does not save a transaction that you are creating. You must run the save config command to save the changes to the stored configuration files.

If, while creating a transaction, you decide you do not want to change the running configuration, you can delete the transaction rather than submit it. However, you can recreate a transaction that you have deleted by using the cli history component. For more information, see page 16-6.
There are a few commands that you can enter on the command line that the system immediately runs, rather than adding the commands to a transaction. These commands are `list` and `show`. Additionally, `tmsh` immediately runs the command sequence `run bigpipe`, but does not add it to the transaction.

**Examples**

The following example shows the syntax that you enter in the `ltm` module to create and submit a transaction that creates a Local Traffic Manager pool and virtual server, and then associates the two.

1. Open `tmsh` batch mode:
   ```
   create /cli transaction
   ```
2. Add a command to the transaction that creates `pool1` for Local Traffic Manager using the default values for a pool:
   ```
   create pool pool1
   ```
3. Add a command to the transaction that creates the virtual server `virtual1` for Local Traffic Manager using the default values for a virtual server and associate it with `pool1`:
   ```
   create virtual virtual1 pool pool1
   ```
4. Display, in a numbered list, the current set of commands in the transaction:
   ```
   list /cli transaction
   ```
   You can use the preceding command to determine the entry ID of a command. Then, you can use this ID to remove or replace a command in the transaction, or to identify a command before which you want to insert another command.
5. Submit the transaction:
   ```
   submit /cli transaction
   ```

**Options**

You can use these options with the `transaction` component:

- **command**
  Specifies, in quotation marks, the full path to a command to add to or delete from the transaction that you are creating. You can also replace an existing command with another command, or insert a command before a command in the transaction.

- **create**
  Opens batch mode.

- **delete**
  Deletes the transaction that you are creating and closes batch mode.

- **list**
  Displays, in a numbered list, the current set of commands in the transaction that you are creating.
◆ **modify**
Specifies a previously entered line in the transaction that you want to change. The options are:

- **delete**
  Deletes the specified entries from the transaction that you are creating.

- **entry_id**
  Specifies the number of a command in the list of commands in the transaction that you want to delete.

◆ **submit**
Submits the transaction that you are entering and closes batch mode. The transaction is submitted in the context of the **cli admin-partitions** settings that are active when the **submit** command is issued.

See also

**cli admin-partitions, create, delete, list, modify, submit, tmsh**
cli alias Module Components

- Introducing the cli alias module
- Alphabetical list of components
Introducing the cli alias module

You can use the `tmsh` components that reside within the `cli alias` module to configure administrative partitions, aliases, and the command line preferences. For more information about the `tmsh` hierarchical structure, see Chapter 2, *Understanding and Using the Traffic Management Shell*.

Alphabetical list of components

The remainder of this chapter lists the `tmsh` components that are available in the `cli alias` module.
private

Configures a user private alias.

Module

cli alias

Syntax

Configure the private component within the cli alias module using the following syntax.

Create/Modify

create private [name]
  options:
    command [commandSyntax]
    command ["command syntax"]
    command "[command syntax]; [command syntax]; ..."
    description [string]
edit private [name]
  options:
    all
modify alias [name]
  options:
    command [commandSyntax]
    command ["command syntax"]
    command "[command syntax]; [command syntax]; ..."

Display

list private
list alias [ [ [name] | [glob] | [regex] ] ... ]
show running-config private
show running-config private [ [ [name] | [glob] | [regex] ] ... ]
  options:
    all-properties
    non-default-properties
    one-line

Delete

delete private [all | [name...name] ]
**Description**

You can use the `private` component to create a shortcut that runs a `tmsh` command sequence. The name of the private alias is what you type on the command line to run the command. If the command sequence for which you are creating an alias contains spaces, it must be enclosed in quotation marks. Command aliases are not case-sensitive.

You can create a private alias that runs multiple commands by entering the command sequences separated by semi-colons. For more information about aliases, see page 2-16.

Private aliases can be used only by the user who created them.

When a batch mode transaction is active, commands that operate on the `private` component are run immediately and are not added to the transaction.

**Examples**

Creates an alias that saves the running configuration in the stored configuration files from anywhere within `tmsh`:

```
create private save command "save config"
```

Creates an alias that displays traffic statistics from anywhere within `tmsh`:

```
create private stats command "show /sys traffic"
```

Creates an alias that displays Local Traffic Manager™ nodes and monitors:

```
create private nodemonitor command "list /ltm node; list /ltm monitor"
```

Creates an alias that displays license and provisioning information:

```
create private myalias command "show /sys provision ; show /sys license"
```

Creates an alias that displays Local Traffic Manager pools from anywhere within `tmsh`:

```
create private ltmpool command "list /ltm pool"
```

**Options**

You can use these options with the `private` component:

- **command syntax**
  Specifies the command to which you are creating an alias. To create an alias that runs multiple commands, type the command sequences separated by semi-colons.

- **description**
  Specifies the purpose of the alias. If you enable `cli preference show-aliases`, `tmsh` displays the description in context-sensitive help.

- **glob**
  Displays the items that match the `glob` expression. For a description of `zglob` expression syntax, see the `glob` man page.
◆ name
  Specifies a name for the alias. This is what you type in **tmsh** to run the command for which you are creating an alias.

◆ regex
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. For a description of regular expression syntax, see the **regex** man page.

**See also**

create, delete, edit, glob, list, modify, regex, show, tmsh
shared

Configures a shared alias.

Module

cli alias

Syntax

Configure the shared alias component within the cli module using the following syntax.

Create/Modify

create shared [name]
  options:
  command [commandSyntax]
  command ["command syntax"]
  command "[command syntax]; [command syntax]; ..."
  description [string]
edit shared [name]
  options:
  all
modify alias [name]
  options:
  command [commandSyntax]
  command ["command syntax"]
  command "[command syntax]; [command syntax]; ...

Display

list shared
list alias [ [ [name] | [glob] | [regex] ] ... ]
show running-config shared
show running-config shared [ [ [name] | [glob] | [regex] ] ... ]
  options:
  all-properties
  non-default-properties
  one-line

Delete

delete shared [all | [name...name] ]
Description

You can use the shared component to create a shortcut to run a \texttt{tmsh} command sequence. The name of the shared alias is what you type on the command line to run the command. If the command sequence for which you are creating an alias contains spaces, it must be enclosed in quotation marks. Command aliases are not case-sensitive.

You can create a shared alias that runs multiple commands by entering the command sequences separated by semi-colons. For more information about aliases, see page 2-16.

Shared aliases can be used by all users.

When a batch mode transaction is active, commands that operate on the \texttt{shared} component are run immediately and are not added to the transaction.

Examples

Creates an alias that saves the running configuration in the stored configuration files from anywhere within \texttt{tmsh}:

\begin{verbatim}
create shared save command "save config"
\end{verbatim}

Creates an alias that displays traffic statistics from anywhere within \texttt{tmsh}:

\begin{verbatim}
create shared stats command "show /sys traffic"
\end{verbatim}

Creates an alias that displays Local Traffic Manager™ nodes and monitors:

\begin{verbatim}
create shared nodemonitor command "list /ltm node; list /ltm monitor"
\end{verbatim}

Creates an alias that displays license and provisioning information.

\begin{verbatim}
create shared myalias command "show /sys provision ; show /sys license"
\end{verbatim}

Creates an alias that displays Local Traffic Manager pools from anywhere within \texttt{tmsh}:

\begin{verbatim}
create shared ltmpool command "list /ltm pool"
\end{verbatim}

Options

You can use these options with the shared alias component:

\begin{itemize}
  \item \textbf{command syntax}
    Specifies the command to which you are creating an alias. To create an alias that runs multiple commands, type the command sequences separated by semi-colons.
  
  \item \textbf{description}
    Specifies the purpose of the alias. If you enable cli preference \texttt{show-aliases}, \texttt{tmsh} displays the description in context-sensitive help.
  
  \item \textbf{glob}
    Displays the items that match the \texttt{glob} expression. See \texttt{help glob} for a description of \texttt{glob} expression syntax.
\end{itemize}
◆ **name**
   Specifies a name for the alias. This is what you type in `tmsh` to run the command for which you are creating an alias.

◆ **regex**
   Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. See `help regex` for a description of regular expression syntax.

See also

create, delete, edit, glob, list, modify, regex, show, tmsh
cm Module Components

- Introducing the cm module
- Alphabetical list of components
Introducing the cm module

You can use the tmsh components that reside within the cm module to manage devices, device groups, and trust relationships. For more information about the tmsh hierarchical structure, see Chapter 2, *Understanding and Using the Traffic Management Shell*.

Alphabetical list of components

The remainder of this chapter lists the tmsh components that are available in the cm module.
cert

Manages a CM trust certificate file.

Module

cm

Syntax

Display or delete the cert component within the cm module using the syntax in the following sections.

Display

list cert
list cert [ [ [name] | [glob] | [regex] ] ... ]

options:
  all-properties
  app-service
  certificate-key-size
  checksum
  create-time
  created-by
  email
  expiration-date
  expiration-string
  fingerprint
  is-bundle
  issuer
  key-type
  last-update-time
  mode
  non-default-properties
  one-line
  partition
  recursive
  revision
  serial-number
  size
  source-path
  subject
  subject-alternative-name
  system-path
Delete

delete cert [name]

Description

You can use the cert component to display or delete a CM trust certificate.

Examples

Displays the CM certificate named new-cert:
list cert new-cert source-path

Deletes the CM certificate named new-cert:
delete cert new-cert source-path

Options

You can use the following options with the cert component:

- **app-service**
  Displays the application service to which the object belongs. The default value is none.

  *Note: If the strict-updates option is enabled on the Application Service that owns the object, you cannot modify or delete the object. Only the Application Service can modify or delete the object.*

- **certificate-key-size**
  Displays the number of bits in the key associated with this certificate.

- **checksum**
  Displays a cryptographic hash or checksum of the file contents for use in verification of file integrity.

- **create-time**
  Displays the time at which the trust certificate was created.

- **created-by**
  Displays the name of the person, who originally created the trust certificate.

- **email**
  Displays the email of the person, who originally created the trust certificate.

- **expiration-date**
  Displays the date at which the trust certificate expires. The date is stored as a POSIX time.
◆ expiration-string
Displays a string representation of the trust certificate expiration date.

◆ fingerprint
Displays the cryptographic fingerprint of the trust certificate.

◆ glob
Displays the items that match the glob expression. See help glob for a description of glob expression syntax.

◆ is-bundle
Indicates whether the trust certificate file is a bundle (that is, whether it contains more than one certificate).

◆ issuer
Displays the X.509 information for the issuer of the trust certificate. If the trust certificate is a bundle, then this displays the issuer information for the primary (first) trust certificate in the bundle.

◆ key-type
Displays the type of cryptographic key associated with this trust certificate.

◆ last-update-time
Displays the last time the trust certificate was modified.

◆ mode
Displays the UNIX® file permissions mode for the file associated with this trust certificate as a numerical value.

◆ partition
Displays the partition within which the trust certificate file resides.

◆ recursive
Displays all objects of the specified type and the folder that contains the object.

◆ regex
Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. See help regex for a description of regular expression syntax.

◆ revision
Displays the number of the latest revision of the trust certificate. The revision starts with 1, and increments on each update.

◆ serial-number
Displays the serial number of the trust certificate.

◆ size
Displays the size (in bytes) of the file associated with the trust certificate.

◆ source-path
Displays the path to the source of the trust certificate, for example:

source-path http://cert-server/cert_store/certs/vs_132.key
source-path https://cert-server/cert_store/certs/vs_132.key
source-path ftp://username:password@server/cert_store/certs/vs_132.key
**subject**
Displays X.509 information about the subject of the trust certificate. If the certificate is a bundle, then the subject information for the primary (first) trust certificate in the bundle displays.

**subject-alternative-name**
Displays a standard X.509 extension as shown in RFC 2459.

**system-path**
Displays the path to the trust certificate.

**updated-by**
Displays the name of the person, who last updated the trust certificate.

**version**
Displays the X.509 version of the trust certificate.

---

**See also**

dele, glob, list, regex, tmsh
config-sync

Manually synchronizes the configuration between devices.

Module

cm

Syntax

Run the config-sync component within the cm module using the syntax in the following section.

Modify

run config-sync
options:
   from-group <name>
   recover-sync
   to-group <name>

Description

You must use only one of the options when you run configuration synchronization. The three options are mutually exclusive.

Examples

Updates the configurations on the remote devices in the device group Common/my_dg with the configuration on the local device. If the local device does not have the newest configuration, then the configuration synchronization does nothing.
run config-sync to-group /Common/my_dg

Updates the configuration on the local device with the configuration from the device in the device group Common/my_dg with the newest configuration. If the local device already has the newest configuration, then the configuration synchronization does nothing.
run config-sync from-group /Common/my_dg

Resets the local device configuration and restores the trust domain, device, and device-group information to default settings.
run config-sync recover-sync
Options

You can use the following options with the `config-sync` command, but only one at a time, because they are mutually exclusive:

- **from-group**
  Updates the configuration of the local device with the configuration of the remote device in the specified device group that has the newest configuration. If the local device already has the newest configuration, then the configuration synchronization does nothing. This option excludes both the `to-group` and `recover-sync` options.

- **recover-sync**
  Resets the local device configuration and restores the trust domain, device, and device-group information to default settings. After this recovery, you can synchronize the configuration of the local device with its peers by running `config-sync` on a peer device and specifying the device group in which the local device is a member. This option excludes both the `from-group` and `to-group` options.

- **to-group**
  Updates the configurations of the remote devices in the specified device group with the configuration of the local device. If the local device does not have the newest configuration, then the configuration synchronization does nothing. This option excludes both the `from-group` and `recover-sync` options.

See also

run, tmsh
device

Manages a device.

Module

cm

Syntax

Manage the **device** component within the **cm** module using the following syntax.

Create/Modify

```plaintext
create device [name]
modify device [name]
```

**options:**
- `comment [string]`
- `configsync-ip [ip address]`
- `contact [string]`
- `description [string]`
- `hostname [string]`
- `location [string]`
- `mirror-ip [ip address]`
- `mirror-secondary-ip [ip address]`
- `multicast-interface [string]`
- `multicast-ip [ip address]`
- `multicast-port [integer]`
- `unicast-address [add | delete | modify | replace-all-with] {unicast address]`

```plaintext
edit device [ [ [name] | [glob] | [regex] ] ... ]
```

**options:**
- `all-properties`
- `non-default-properties`

Display

```plaintext
list device
list device [ [ [name] | [glob] | [regex] ] ... ]
```

**options:**
- `active-modules`
- `all-properties`
- `app-service`
- `base-mac`
You can use the `device` component to manage devices.

**WARNING**

*F5 Networks recommends that you do not create or delete devices. Instead, to add or remove devices on the BIG-IP® system, modify the Root trust domain. For more information, see the `help trust-domain`.*

**Options**

You can use the following options with the `device` component:

- **active-modules**
  
  Displays the licensed modules that are currently active on the device.
- **app-service**
  Displays the application service to which the object belongs. The default value is **none**.

  *Note: If the strict-updates option is enabled on the Application Service that owns the object, you cannot modify or delete the object. Only the Application Service can modify or delete the object.*

- **base-mac**
  Displays the base MAC address for the device.

- **build**
  Displays the software build number.

- **cert**
  Displays the identity certificate used for device trust.

- **chassis-id**
  Displays the chassis identifier.

- **chassis-type**
  Displays the chassis type. The possible values are **individual** and **viprion**.

- **comment**
  Specifies user comments about the device.

- **configsync-ip**
  Specifies the IP address used for configuration synchronization. If you specify a self IP address, the self IP address object must be located in the **Common** folder.

- **contact**
  Specifies administrator contact information.

- **description**
  Specifies a user-defined description of the device.

- **edition**
  Displays the software edition.

- **failover-state**
  Displays the device failover state.

- **glob**
  Displays the items that match the **glob** expression. See help glob for a description of **glob** expression syntax.

- **hostname**
  Specifies a host name for the device.

- **inactive-modules**
  Displays the licensed modules that are currently inactive on the device.

- **key**
  Displays the identity key used for device trust.

- **location**
  Specifies the physical location of the device.

- **marketing-name**
  Displays the marketing name of the device platform.
◆ **mirror-ip**  
Specifies the IP address used for state mirroring. If you specify a self IP address, the self IP address object must be located in the Common folder.

◆ **mirror-secondary-ip**  
Specifies the secondary IP address used for state mirroring. If you specify a self IP address, the self IP address object must be located in the Common folder.

◆ **multicast-interface**  
Specifies the interface name used for the failover multicast IP address.

◆ **multicast-ip**  
Specifies the multicast IP address used for failover.

◆ **multicast-port**  
Specifies the multicast port used for failover.

◆ **optional-modules**  
Displays the modules that are available for the current platform, but are not currently licensed.

◆ **platform-id**  
Displays the device platform identifier.

◆ **product**  
Displays the software product name.

◆ **recursive**  
Displays all objects of the specified type and the folder that contains the object.

◆ **regex**  
Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. See *help regex* for a description of regular expression syntax.

◆ **self-device**  
Displays true, when the device is the self device.

◆ **time-limited-modules**  
Displays the licensed modules that are time-limited.

◆ **time-zone**  
Displays the time zone configured on the device.

◆ **unicast-address**  
Displays the set of unicast IP addresses used for failover. If you specify a self IP address, the self IP address object must be located in the Common folder.

◆ **version**  
Displays the software version number.

See also

create, delete, edit, glob, list, modify, regex, show, tmsh, trust-domain
device-group

Configures device groups.

Module

cm

Syntax

Modify the device-group component within the cm module using the syntax shown in the following sections.

Create/Modify

create device-group [name]
modify device-group [name]

options:
asm-sync [ enabled | disabled ]
auto-sync [ enabled | disabled ]
description [string]
devices [add | delete | modify | replace-all-with] {
  [ device_name ]
}full-load-on-sync [true | false]
network-failover [ enabled | disabled ]
type [ sync-only | sync-failover ]

edit device-group [ [ [name] | [glob] | [regex] ] ... ]

options:
  all-properties
  non-default-properties

Display

list device-group

list device-group [ [ [name] | [glob] | [regex] ] ... ]

show running-config device-group

show running-config device-group [ [ [name] | [glob] | [regex] ] ... ]

options:
all-properties
app-service
non-default-properties
partition
recursive

show device-group

show device-group [name]

options:
  field-fmt
Delete

delete device-group [name]

◆ Note

The device group must be empty, and you must remove all references to the device group, before you can delete the device group.

Description

You can use the device-group component to manage sets of devices used for configuration synchronization and failover.

Examples

create device-group my_device_group devices add {
    /Common/device1
    /Common/device2
}

Creates a sync-only device group named my_device_group with two devices, device1 and device2.

delete device-group my_device_group

Deletes the device group named my_device_group.

list device-group my_device_group

Displays properties of the the device group named my_device_group.

Options

◆ app-service
   Displays the application service to which the object belongs. The default value is none. Note: If the strict-updates option is enabled on the Application Service that owns the object, you cannot modify or delete the object. Only the Application Service can modify or delete the object.

◆ asm-sync
   Specifies whether to synchronize ASM configurations of device group members. The default value is disabled. A device can be a member of only one ASM-enabled device group.

◆ auto-sync
   Specifies whether the device group automatically synchronizes configuration data to its members. The default value is disabled.

◆ description
   Specifies a user-defined description of the device group.
- **devices**
  Adds, deletes, or replaces a set of devices to a device group by specifying the device name(s). When the local device is removed from a device group then all of the sys folders that are associated with the device group are reset to have no device group and the name of each folder that was updated is logged to /var/log/ltm.

- **full-load-on-sync**
  Specifies that the entire configuration for a device group is sent when configuration synchronization is performed. The default value is true.

- **glob**
  Displays the items that match the glob expression. See help glob for a description of glob expression syntax.

- **name**
  Specifies a unique name for the component. This option is required for the commands create, delete, and modify.

- **network-failover**
  When the device group type is failover, specifies whether network failover is used.

- **partition**
  Displays the administrative partition within which the device group resides.

- **recursive**
  Displays all objects of the specified type and the folder that contains the object.

- **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. See help regex for a description of regular expression syntax.

- **type**
  Specifies the type of device group. You can use this option only when you create a device group. You cannot modify the type of a device group. The default value is sync-only.

**See Also**

create, delete, device, edit, glob, list, modify, regex, tmsh
failover-status

Displays the failover status of the local device.

Module

cm

Syntax

Use the failover-status component within the cm module using the following syntax.

Display

```
show failover-status
  option:
    field-fmt
```

Description

You can use the failover-status component to display the failover status of the local device.

◆ Note

For information about the options that you can use with the command show, run the command sequence help show.

Example

Displays the failover status of the local device.

```
show failover-status
```

See Also

```
show, tmsh
```
Manages a CM trust certificate private key file.

Module

cm

Syntax

Display or delete a key component within the cm module using the syntax shown in the following sections.

Display

list key
list key [ [ name ] | [ glob ] | [ regex ] ] ...

options:
  all-properties
  app-service
  checksum
  create-time
  created-by
  key-size
  key-type
  last-update-time
  mode
  non-default-properties
  one-line
  partition
  recursive
  revision
  security-type
  size
  source-path
  system-path
  updated-by

Delete

delete key [ name ]
Description

You can use the `key` component to display or delete a certificate key.

Examples

Displays the CM key named `new-key`:

```
list key new-key
```

Deletes the CM key named `new-key`:

```
delete key new-key
```

Options

You can use the following options with the `key` component:

- **app-service**
  Displays the application service to which the object belongs. The default value is `none`.

  **Note:** If the `strict-updates` option is enabled on the Application Service that owns the object, you cannot modify or delete the object. Only the Application Service can modify or delete the object.

- **checksum**
  Displays a cryptographic hash or checksum of the key for use in verification of key integrity.

- **create-time**
  Displays the time at which the key was created.

- **created-by**
  Displays the user who originally created the key.

- **glob**
  Displays the items that match the `glob` expression. See `help glob` for a description of `glob` expression syntax.

- **key-size**
  Displays the size of the cryptographic key, in bits.

- **key-type**
  Displays the cryptographic algorithm that this key is compatible with. A key can be one of two types:

  - **rsa-private**
    The key is an RSA private key.

  - **dsa-private**
    The key is a DSA-based private key.

- **last-update-time**
  Displays the time at which the key was last modified.

- **mode**
  Specifies the UNIX file permissions mode for the file associated with this file-object as a numerical value.
◆ name
   Specifies the name of the key you want to delete.

◆ partition
   Displays the partition within which the key resides.

◆ recursive
   Displays all objects of the specified type and the folder that contains the object.

◆ regex
   Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. See help regex for a description of regular expression syntax.

◆ revision
   Displays the latest revision of the key. The revision starts with 1, and increments on each update.

◆ security-type
   Displays the type of security used to handle or store the key. There are three mutually exclusive options:
   • normal
     Indicates that the key resides in a standard form on the file-system. This is the default security type.
   • fips
     Indicates that the key is protected by a FIPS device on the system, and is only applicable to devices with FIPS support.
   • password
     Indicates that the key is protected by a passphrase and stored in encrypted form.

◆ size
   Displays the size (in bytes) of the file associated with this key.

◆ source-path
   Displays the path to the source of the key. This option takes a URL, for example:

source-path http://cert-server/cert_store/certs/vs_132.key
source-path https://cert-server/cert_store/certs/vs_132.key
source-path ftp://username:password@server/cert_store/certs/vs_132.key

◆ system-path
   Displays the location where the key is stored on the system.

◆ updated-by
   Displays the name of the user who last updated the key.

See also

dele, glob, list, regex, tmsh
**sniff-updates**

Displays the commit ID updates that occur over the CMI communications channel.

### Module

**cm**

### Syntax

Run the `sniff-updates` component within the **cm** module using the following syntax.

```plaintext
run sniff-updates
```

#### Options

You can use the following option when you run the `sniff-updates` component:

- `-v`
  
  Formats the update output using fully qualified device and device group names, and exact `time64_t` timestamps.

### Description

You can use the `sniff-updates` component to monitor the internal CMI communications channel for commit ID updates. The system displays each update as it arrives, one per line.

```
[15:35:57] bigip1 (v0.0.0) device_trust_group: CID 105 bigip2 at 15:34:39 FORCE_SYNC
```

**Table 18.1 Output fields defined**

### Options

You can use the following option when you run the `sniff-updates` component:

- `-v`
  
  Formats the update output using fully qualified device and device group names, and exact `time64_t` timestamps.
See Also

run, tmsh
sync-status

Displays the configuration synchronization status of the local device.

Module

cm

Syntax

Run the sync-status component within the cm module using the following syntax.

Display

```
show sync-status
options:
  field-fmt
```

Description

You can use the sync-status component to display the configuration synchronization status of the local device.

◆ Note

For information about the options that you can use with the command show, run the command sequence help show.

Examples

Displays the configuration synchronization status of the local device:

```
show sync-status
```

Options

You can use the following option when you run the sync-status component:

◆ field-fmt
  Formats the status output in command syntax.

See Also

show, tmsh
traffic-group

Manages a CM traffic group.

Module

cm

Syntax

Manage the traffic-group component within the cm module using the syntax shown in the following sections.

Create/Modify

create traffic-group [name]
modify traffic-group [name]
  options:
    auto-failback-enabled [ enabled | disabled ]
    auto-failback-time [ integer ]
    default-device [ string ]
    description [string ]
    mac [mac address]
edit traffic-group [ [ [name] | [glob] | [regex] ] ... ]
  options:
    all-properties
    non-default-properties

Display

list traffic-group
list traffic-group [ [ [name] | [glob] | [regex] ] ... ]
show running-config traffic-group
show running-config traffic-group [ [ [name] | [glob] | [regex] ] ... ]
  options:
    all-properties
    app-service
    is-floating
    non-default-properties
    one-line
    partition
    recursive
    unit-id [integer]
show traffic-group
show traffic-group [name]
options:
    all-properties
    field-fmt

Delete

delete traffic-group [name]

Description

You can use the traffic-group component to specify the failover behavior for devices in a failover device group.

Examples

Creates a traffic group named my_traffic_group:
create traffic-group my_traffic_group

Creates a traffic group named my_traffic_group with a default device named my_device:
create traffic-group my_traffic_group default-device my_device

Options

You can use the following options with the traffic-group component.

◆ app-service
    Displays the application service to which the object belongs. The default value is none.
    
    Note: If the strict-updates option is enabled on the Application Service that owns the object, you cannot modify or delete the object. Only the Application Service can modify or delete the object.

◆ auto-failback-enabled
    Specifies whether the traffic group fails back to the default device.

◆ auto-failback-time
    Specifies the time required to fail back. The value must be within a valid range: 0 - 300 inclusive.

◆ default-device
    Specifies the default active device for this traffic group.

◆ description
    Specifies a user-defined description.

◆ glob
    Displays the items that match the glob expression. See help glob for a description of glob expression syntax.
◆ **is-floating**
   Indicates whether the traffic group can fail over to other devices in the device group.

◆ **mac**
   Specifies a MAC address for the traffic group.

◆ **partition**
   Displays the administrative partition within which the device group resides.

◆ **recursive**
   Displays all objects of the specified type and the folder that contains the object.

◆ **regex**
   Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. See `help regex` for a description of regular expression syntax.

◆ **unit_id**
   Displays the unit ID for the traffic group. The unit ID is set automatically when you create a traffic group. The value is between 1 and 15.

**See also**

`create, delete, edit, glob, list, modify, regex, tmsh`
trust-domain

Manages a CM trust domain by providing control of object failover.

Module

cm

Syntax

Manage the trust-domain component within the cm module using the syntax shown in the following sections.

Create/Modify

create trust-domain [name]
modify trust-domain [name]

options:
  ca-devices [add | delete | modify | replace-all-with] {
    [ device_name | ip address ]
  }
md5-fingerprint [string]
name [string]
non-ca-devices [add | delete | modify | replace-all-with] {
    [ device_name | ip address ]
  }
password [string]
save-on-auto-sync
serial [string]
sha1-fingerprint [string]
signature [string]
username [string]

Display

list trust-domain
list trust-domain [ [ [name] | [glob] | [regex] ] ... ]
  all-properties
  app-service
  ca-cert
  ca-cert-bundle
  ca-key
  non-default-properties
  one-line
Delete

delete trust-domain [name]

Description

You can use the trust-domain component to manage the behavior of objects during failover.

Examples

Adds a certificate authority:

```
modify trust-domain Root ca-devices add { 192.168.1.245 } name myDevice1 username admin password admin
```

Adds a non-authoritative certificate:

```
modify trust-domain Root non-ca-devices add { 192.168.1.245 } name myDevice1 username admin password admin
```

Removes a device from the trust domain:

```
modify trust-domain Root ca-devices delete { myDevice1 }
```

Options

You can use the following options with the trust-domain component:

- **app-service**
  Displays the application service to which the object belongs. The default value is none.

  *Note: If the strict-updates option is enabled on the Application Service that owns the object, you cannot modify or delete the object. Only the Application Service can modify or delete the object.*

- **ca-cert**
  Displays the certificate authority device trust certificate.

- **ca-cert-bundle**
  Displays the bundled certificate authority device trust certificates used to authenticate incoming connections.

- **ca-devices**
  Specifies a set of certificate authority devices in the trust domain.
- **ca-key**
  Displays the certificate authority device trust key. This key only displays for certificate authorities.

- **glob**
  Displays the items that match the `glob` expression. See `help glob` for a description of `glob` expression syntax.

- **md5-fingerprint**
  Specifies the SSL certificate fingerprint when verifying the identity of a new device.

- **name**
  Specifies the name of a device.

- **non-ca-devices**
  Specifies a set of subordinate devices in the trust domain.

- **password**
  Specifies the password for a new device.

- **recursive**
  Displays all objects of the specified type and the folder that contains the object.

- **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. See `help regex` for a description of regular expression syntax.

- **save-on-auto-sync**
  Specifies whether to save the configuration on the remote devices following an automatic configuration synchronization.

  *Note: This value applies to all device groups, in this trust domain, that are configured for automatic synchronization.*

- **serial**
  Specifies the SSL certificate serial number when verifying the identity of a new device.

- **sha1-fingerprint**
  Specifies the SSL certificate fingerprint when verifying the identity of a new device.

- **signature**
  Specifies the SSL certificate signature, when verifying the identity of a new device.

- **status**
  Displays the status of the trust domain.

- **trust-group**
  Displays the device group associated with the trust domain.

- **username**
  Specifies the user name required to log on to a device when adding the device to the trust domain.
See also

create, delete, edit, glob, list, modify, regex, tmsh
watch-devicegroup-device

Displays information about the devices in the device group to which the local device belongs.

Module

cm

Syntax

Run the watch-devicegroup-device component within the cm module using the following syntax.

Run

run watch-devicegroup-device

Display

By default, multiple devices with identical information are collapsed into a single row that displays in green. The devices column identifies the devices by the suffix of the configuration synchronization IP address configured on the device. For example, if the devices in a device group have the IP addresses 10.0.0.15 and 10.0.0.16, the IDs in this column will be 15 and 16. You can use the e (collapse) command to deactivate/activate this behavior.

Description

You can use the watch-devicegroup-device component to view dynamic information about the synchronization of the devices in the device group to which the local device belongs. You can use this information to monitor or troubleshoot the devices.

For example, when you make a change to a device, the change is identified by a commit ID (cid.id) that displays when you run the watch-devicegroup-device component.

Within the component, you can use the following keys:

- Press h to see a list of available commands.
- Press the back tick key (\`) to exit the help page.
- Press c to toggle the view from a collapsed view to a full view. The command gathers information from every device in the trust group. When all devices in the trust group report the same information the view is collapsed and one line, highlighted in green, displays the information.
The devices included in the line are shown in the devices column. You can press the <c> key to see the full view, which displays each device on a separate line.

- Press Ctrl-C to exit the component.
- Press the arrow keys to navigate across the columns or down the rows.

<table>
<thead>
<tr>
<th>Column name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>devices</td>
<td>Displays the suffix of the configuration synchronization IP address configured on the device. For example, if the devices in a device group have the configuration synchronization IP addresses 10.0.0.15 and 10.0.0.16, the IDs in this column will be 15 and 16.</td>
</tr>
<tr>
<td>devgroup</td>
<td>Displays the name of the device group to which the device belongs.</td>
</tr>
<tr>
<td>device</td>
<td>Displays the device name.</td>
</tr>
<tr>
<td>cid.id</td>
<td>Displays the commit ID, which is a configuration change identifier.</td>
</tr>
<tr>
<td>cid.orig</td>
<td>Displays the name of the device on which the configuration change was made.</td>
</tr>
<tr>
<td>cid.time</td>
<td>Displays the time the configuration change was made.</td>
</tr>
<tr>
<td>last_sync</td>
<td>Displays the time the device configuration was last synchronized with the device group. The devices in the to-group of a configuration synchronization display the same time in this column. The local device that pushes the configuration to the other devices in the device group (to-group) has a different value in this column. The devices in the from-group of a configuration synchronization display the same time in this column. The local device that receives the configuration from the other devices has a different value in this column. You can use this information to determine a rollback strategy.</td>
</tr>
</tbody>
</table>

| Table 18.2 Data in watch-devicegroup-device component output |

**See Also**

run, tmsh, watch-sys-device, watch-trafficgroup-device
watch-sys-device

Displays information about the local device.

Module
cm

Syntax

Run the `watch-sys-device` component within the `cm` module using the following syntax.

Run

`run watch-sys-device`

Display

By default, multiple devices with identical information are collapsed into a single row that displays in green. The devices column identifies the devices by the suffix of the configuration synchronization IP address configured on the device. For example, if the devices in a device group have the IP addresses `10.0.0.15` and `10.0.0.16`, the IDs in this column will be `15` and `16`. You can use the `c` (collapse) command to deactivate/activate this behavior.

Description

You can use the `watch-sys-device` component to view dynamic information about the local device.

Within the component, you can use the following keys:

- Press `h` to see a list of available commands.
- Press the back tick key (`) to exit the help page.
- Press `c` to toggle the view from a collapsed view to a full view. The command gathers information from every device in the trust group. When all devices in the trust group report the same information the view is collapsed and one line, highlighted in green, displays the information. The devices included in the line are shown in the devices column. You can press the `c` key to see the full view, which displays each device on a separate line.
- Press `Ctrl-C` to exit the component.
- Press the arrow keys to navigate across the columns or down the rows.
### Table 18.3 Data in watch-sys-device component output

<table>
<thead>
<tr>
<th>Column name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>devices</td>
<td>Displays the suffix of the configuration synchronization IP address configured on the device. For example, if the devices in a device group have the IP addresses <code>10.0.0.15</code> and <code>10.0.0.16</code>, the IDs in this column will be <code>15</code> and <code>16</code>.</td>
</tr>
<tr>
<td>name</td>
<td>Displays the device name.</td>
</tr>
<tr>
<td>platform</td>
<td>Displays the device platform.</td>
</tr>
<tr>
<td>build</td>
<td>Displays the software build installed on the device.</td>
</tr>
<tr>
<td>failover_state</td>
<td>Displays the high availability state (active or standby) of the device.</td>
</tr>
<tr>
<td>mgmt_ip</td>
<td>Displays the IP address of the management port on the device.</td>
</tr>
<tr>
<td>confgsync_ip</td>
<td>Displays the IP address on the device that is used for configuration synchronization.</td>
</tr>
<tr>
<td>unicast_ip</td>
<td>Displays the unicast IP address of the device.</td>
</tr>
<tr>
<td>multicast_ip</td>
<td>Displays the multicast IP address of the device.</td>
</tr>
<tr>
<td>mirror_ip</td>
<td>Displays the IP address used for configuration mirroring for the device.</td>
</tr>
<tr>
<td>mirror_secondary_ip</td>
<td>Displays the secondary IP address used for configuration mirroring for the device.</td>
</tr>
<tr>
<td>desc</td>
<td>Displays a description of the device.</td>
</tr>
</tbody>
</table>

### See Also

run, tmsh, watch-devicegroup-device, watch-trafficgroup-device
**watch-trafficgroup-device**

Displays information about the traffic groups associated with devices in a device group.

**Module**

`cm`

**Syntax**

Run the `watch-trafficgroup-device` component within the `cm` module using the following syntax.

**Run**

`run watch-trafficgroup-device`

**Display**

By default, multiple devices with identical information are collapsed into a single row that displays in green. The devices column identifies the devices by the suffix of the configuration synchronization IP address configured on the device. For example, if the devices in a device group have the IP addresses `10.0.0.15` and `10.0.0.16`, the IDs in this column will be `15` and `16`. You can use the `c` (collapse) command to deactivate/activate this behavior.

**Description**

You can use the `watch-trafficgroup-device` component to view dynamic information about the failover status of the devices in a device group to which the local device belongs. You can use this information to monitor or troubleshoot the devices in the device group.

Within the component, you can use the following keys:

- Press `h` to see a list of available commands.
- Press the back tick key (`) to exit the help page.
- Press `c` to toggle the view from a collapsed view to a full view. The command gathers information from every device in the device group. When all devices in the device group report the same information the view is collapsed and one line, highlighted in green, displays the information. The devices included in the line are shown in the devices column. You can press the `c` key to see the full view, which displays each device on a separate line.
- Press `Ctrl-C` to exit the component.
- Press the arrow keys to navigate across the columns or down the rows.
### Table 18.4 Data in watch-trafficgroup-device component output

<table>
<thead>
<tr>
<th>Column name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>devices</td>
<td>Displays the suffix of the configuration synchronization IP address configured on the device. For example, if the devices in a device group have the IP addresses 10.0.0.15 and 10.0.0.16, the IDs in this column will be 15 and 16.</td>
</tr>
<tr>
<td>traffic_group</td>
<td>Displays the name of the traffic group associated with the device.</td>
</tr>
<tr>
<td>device_name</td>
<td>Displays the device name.</td>
</tr>
<tr>
<td>failover_state</td>
<td>Displays the high availability state (active or standby) of the device.</td>
</tr>
<tr>
<td>next_active</td>
<td>Displays <strong>TRUE</strong> for the device that becomes active if the active traffic group fails over.</td>
</tr>
<tr>
<td>score</td>
<td>Displays a system-generated high availability score used to select the next active device.</td>
</tr>
</tbody>
</table>

**See Also**

- run
- tmsh
- watch-devicegroup-device
- watch-sys-device
gtm Module Components

- Introducing the gtm module
- Alphabetical list of components
Introducing the gtm module

You can use the \texttt{tmsh} components that reside within the \texttt{gtm} module to configure Global Traffic Manager™. For more information about the \texttt{tmsh} hierarchical structure, see Chapter 2, \textit{Understanding and Using the Traffic Management Shell}.

Alphabetical list of components

The remainder of this chapter lists the \texttt{tmsh} components that are available in the \texttt{gtm} module.
datacenter

Configures a Global Traffic Manager™ data center.

Module

gtm

Syntax

Configure the datacenter component within the gtm module using the following syntax.

Create/Modify

create datacenter [name]
modify datacenter [name]
options:
  contact [ [name] | none]
  description [string]
  [disabled | enabled]
  location [none | [physical location] ]
  metadata [add | delete | modify] {
    [metadata_name ... ] {
      value [ "value content" ]
      persist [ true | false ]
    }
  }
  prober-pool [none | name]
edit datacente r [ [ [name] | [glob] | [regex] ] ... ]
options:
  all-properties
  non-default-properties
  one-line
reset-stats datacenter
reset-stats datacenter [name]

Display

list datacenter
list datacenter [ [ [name] | [glob] | [regex] ] ... ]
show running-config datacenter
show running-config datacenter [ [ [name] | [glob] | [regex] ] ... ]
options:
**Datacenter Component**

You can use the `datacenter` component to create, modify, display, or delete a data center.

**Important**

*The name of a data center must be no more than 63 characters in length.*

**Examples**

Creates a data center named **DC1** with options set to the default values:

```
create datacenter DC1
```

Displays all properties of the data center named **DC1**:

```
list datacenter DC1 all-properties
```

**Options**

You can use these options with the `datacenter` component:

- **contact**
  
  Specifies the name of the administrator or the name of the department that manages the data center. The default value is **none**.

- **description**
  
  User-defined description.

- **[disabled | enabled]**
  
  Specifies whether the data center and its resources are available for load balancing. The default value is **enabled**.

- **glob**
  
  Displays the items that match the **glob** expression. For a description of **glob** expression syntax, see the **glob** man page.
◆ location
  Specifies the physical location of the data center. The default value is none.
◆ metadata
  Specifies user-defined data to associate with a server. By default the persist attribute is set to true. This means the data is saved into the configuration file.
◆ name
  Specifies a unique name for the component. This option is required for the create and modify commands.
◆ prober-pool
  Specifies a prober pool to use to monitor servers defined in this data center.
◆ regex
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. For a description of regular expression syntax, see the regex man page.

See also

create, delete, glob, gtm link, gtm prober-pool, gtm server, list, modify, regex, reset-stats, show, tmsh
distributed-app

Configures a Global Traffic Manager distributed application.

Module

gtm

Syntax

Configure the distributed-app component within the gtm module using the following syntax.

Create/Modify

create distributed-app [name]
modify distributed-app [name]

options:
  dependency-level [datacenter | link | none | server | wideip]
  description [string]
  disabled-contexts
    [add | delete | modify | replace-all-with] {
      [datacenter | link | server | [name] ... ]
    }
  disabled-contexts none
  persistence [enabled | disabled]
  ttl-persistence [integer]
  wideips
    [add | delete | replace-all-with] {
      [name] ... 
    }
  wideips [default | none]

edit distributed-app [ [ name ] | [ glob ] | [ regex ] ] ... ]

options:
  all-properties
  non-default-properties

reset-stats distributed-app
reset-stats distributed-app [ [ name ] | [ glob ] | [ regex ] ] ... ]

options:
  all-properties
  non-default-properties
  one-line
Display

list distributed-app
list distributed-app [ [ name ] | [ glob ] | [ regex ] ]...
show running-config distributed-app
show running-config distributed-app [ [ name ] | [ glob ] | [ regex ] ]...
  options:
    all-properties
    non-default-properties
    one-line
    partition
show distributed-app
show distributed-app [ name ]
  options:
    (default | exa | gig | kil | meg | peta | raw | tera | yotta | zetta)
    detail
    field-fmt

Delete

delete distributed-app [ name ]

Description

You can use the distributed-app component to create, modify, display, or delete a distributed application.

Examples

Creates a distributed application named DA1 with options set to the default values:
create distributed-app DA1

Displays all properties of the distributed application named DA1:
list distributed-app DA1 all-properties
Options

You can use these options with the `distributed-app` component:

- **dependency-level**
  Specifies the resources that must be in the available state before this distributed application is considered available.
  The options are:
  - **datacenter**
    All of the data centers on the member list of this distributed application must be in an available state before the system considers the distributed application available.
  - **link**
    All of the links on the member list of this distributed application must be in an available state before the system considers the distributed application available.
  - **none**
    The distributed application has no dependencies. This value effectively disables this option. This is the default value.
  - **server**
    All of the servers on the member list of this distributed application must be in an available state before the system considers the distributed application available.
  - **wideip**
    All of the wideips on the member list of this distributed application must be in an available state before the system considers the distributed application available.

- **description**
  User-defined description.

- **disabled-contexts**
  Specifies the components that you want to add to or delete from this distributed application as disabled-contexts. You can also replace all of the components that are currently listed as disabled-contexts for this distributed application with other components. The default value is **none**.
  The possible values are:
  - **datacenter**
    Specifies the datacenters, by name, to which the system does not send traffic from this distributed application.
  - **link**
    Specifies the links, by name, to which the system does not send traffic from this distributed application.
  - **none**
    There are no components to which the system does not send traffic from this distributed application. This value effectively disables this option.
  - **server**
    Specifies the servers, by name, to which the system does not send traffic from this distributed application.
◆ **glob**
Displays the items that match the *glob* expression. For a description of the *glob* expression syntax, see the *glob* man page.

◆ **name**
Specifies a unique name for the component. This option is required for the *create* and *modify* commands.

◆ **partition**
Displays the administrative partition within which this object resides.

◆ **persistence**
When *enabled*, if a local DNS server makes repetitive requests on behalf of a client, the system reconnects the client to the same resource as previous requests. The default value is *disabled*.

◆ **regex**
Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. For a description of regular expression syntax, see the *regex* man page.

◆ **ttl-persistence**
Specifies, in seconds, the length of time for which the persistence entry is valid. The default value is 3600.

◆ **wideips**
Specifies the wide IPs, by name, that you want to add to or delete from this distributed application. You can also replace all of the wide IPs that are currently associated with this distributed application with other wide IPs. The default value is *none*.

A *wide IP* is a collection of one or more domain names that maps to one or more groups of virtual servers managed either by BIG-IP® systems or by host servers. The Global Traffic Manager load balances name resolution requests across the virtual servers that are defined in the wide IP that is associated with the requested domain name.

See also

create, delete, glob, gtm link, gtm server, list, modify, regex, reset-stats, show, tmsh
**iquery**

Displays information about iQuery.

**Module**

gtm

**Syntax**

Configure the `iquery` component within the `gtm` module using the following syntax.

**Display**

```bash
show iquery
```

**options:**

- (default | exa | gig | kil | meg | peta | raw | tera | yotta | zetta)
- field-fmt
- global

**Description**

You can use the `iquery` component to display iQuery statistics.

**Examples**

Displays iQuery statistics in the system default units:

```bash
show iquery
```

Displays iQuery statistics in field format:

```bash
show iquery field-fmt
```

**Options**

For information about options for the `show` command, see `show`, on page 3-39.

**See also**

`show`, `tmsh`
ldns

Displays local domain name system (LDNS) statistics for the Global Traffic Manager.

Module

gtm

Syntax

Configure the ldns component within the gtm module using the following syntax.

Display

show ldns

options:
(default | gig | kil | meg | raw)

field-fmt

Description

You can use the ldns component to display LDNS statistics.

Examples

Displays LDNS statistics in the system default units:
show ldns

Displays LDNS statistics in field format:
show ldns field-fmt

Options

For information about options for the show command, see show, on page 3-39.

See also

show, tmsh
link

Configures Global Traffic Manager links.

Module

gtm

Syntax

Configure the link component within the gtm module using the following syntax.

Create/Modify

create link [name]
modify link [name]

options:

  cost-segments {
    { [up-to-bps [integer] ] [dollars-per-mbps [integer] ] } ... 
  }
datacenter [string]
description [string]
[disabled | enabled]
duplex-billing [disabled | enabled]
limit-max-inbound-bps [integer]
limit-max-inbound-bps-status [disabled | enabled]
limit-max-outbound-bps [integer]
limit-max-outbound-bps-status [disabled | enabled]
limit-max-total-bps [integer]
limit-max-total-bps-status [disabled | enabled]
link-ratio [integer]
monitor [ [name] | none]
prepaid-segment [integer]
router-addresses
  [add | delete | modify | replace-all-with] {
    [ip address] {
      translation [disabled | enabled]
      device-name [name] 
    }
  }

service-provider [name]
uplink-address [ip address]
weighting [price | ratio]
edit link [ [name | glob | regex] ... ]

options:
Chapter 19

all-properties
non-default-properties
one-line
reset-stats link
reset-stats link [ [name | glob | regex] ... ]

Display

list link
list link [name]
show running-config link
show running-config link [name]
    options:
        all-properties
        non-default-properties
show link
show link [name]
    options:
        (default | gig | kil | meg | raw)
        field_fmt

Delete

delete link [name]

Description

You can use the link component to create, display, modify, or delete a link. A link is a logical representation of a physical device (router) that connects your network to the Internet. You can attach links to a collection of servers to manage access to the data sources on the network.

Important

The name of a link must be no more than 63 characters in length.

Examples

Creates a link named my_link in the DC1 data center and adds the IP address of the router that uses this link:

create link my_link datacenter DC1 router-addresses add {10.10.1.1}

Displays all non-default properties for all links:

list link non-default-properties
Options

You can use these options with the link component:

- **cost-segments**
  Specifies the cost of each incremental segment of bandwidth. This option is valid only when the weighting option is set to price.

  **Note:** You cannot modify the list. You can only replace all of the options in the list.

  By default, the list is empty.

  The options are:
  - **dollars-per-mps**
    Specifies the cost in dollars per megabytes per second. By default this value is not specified.
  - **up-to-bps**
    Specifies the cost in dollars per bytes per second. By default this value is not specified.

- **datacenter**
  Specifies the data center to which the link belongs.

- **description**
  User-defined description.

- **[disabled | enabled]**
  Specifies whether the link and its resources are available for load balancing. The default value is enabled.

- **duplex-billing**
  Enables or disables duplex billing for this link. The default value is enabled. This option is valid only when the weighting option is set to price.

  The options are:
  - **disabled**
    The internet service provider (ISP) that supplies this link bills for bandwidth usage based on the total amount of inbound plus outbound traffic on the link.
  - **enabled**
    The ISP that supplies this link bills for bandwidth usage based on the maximum amount of either inbound or outbound traffic on the link (whichever is higher), rather than billing for bandwidth usage based on the total amount of inbound plus outbound traffic on the link.

- **glob**
  Displays the items that match the glob expression. For a description of glob expression syntax, see the glob man page.

- **limit-max-inbound-bps**
  Specifies the threshold for inbound traffic on the link. The default value is 0 (zero).

- **limit-max-inbound-bps-status**
  Enables or disables the limit-max-inbound-bps option for this link. The default value is disabled.
◆ limit-max-outbound-bps
   Specifies the threshold for inbound traffic on the link. The default value
   is 0 (zero).

◆ limit-max-outbound-bps-status
   Enables or disables the limit-max-outbound-bps option for this link.
   The default value is disabled.

◆ limit-max-total-bps
   Specifies the threshold as a sum of inbound and outbound traffic on the
   link. The default value is 0 (zero).

◆ limit-max-total-bps-status
   Enables or disables the limit-max-total-bps option for this link. The
   default value is disabled.

◆ link-ratio
   Specifies the frequency at which the system sends traffic through the
   link. The default value is 1.
   
   Important: When you set this option, you must also set the weighting
   option to ratio.

◆ monitor
   Specifies the health monitors that the system uses to determine whether
   this link is available for load balancing. The default value is none.

◆ name
   Specifies a unique name for the component. This option is required for
   the create and modify commands.

◆ prepaid-segment
   Specifies the amount of bandwidth for which the system is prepaid. This
   option is valid only when the weighting option is set to price. The
   default value is 0 (zero).

◆ regex
   Displays the items that match the regular expression. The regular
   expression must be preceded by an at sign (@[regular expression]) to
   indicate that the identifier is a regular expression. For a description of
   regular expression syntax, see the regex man page.

◆ router-addresses
   Specifies the IP addresses of the routers that use this link. A router
   address can be associated with only one link. You can use the following
   options.

   • translation
     Specifies the address that the link uses for translation when
     communicating between the network and the Internet. The default
     value is any6.

   • device-name
     Specifies the name of this system in a redundant system
     configuration. The default value is the link name.
◆ **uplink-address**  
Specifies the IP address the system uses to gather Simple Network Management Protocol (SNMP) metrics from the router interface. When you configure an uplink address, the system sends SNMP requests to the IP addresses configured using the `router-addresses` option for this link.

◆ **weighting**  
Specifies the weighting methodology the system uses to select a link to which to send traffic. The default value is **ratio**.

The options are:

- **price**  
The system continuously checks the performance of each link and sends traffic through the link with the best performance data.

- **ratio**  
The system uses the value that you set in the `link-ratio` option to determine the link to which to send traffic.

---

**See also**

create, delete, edit, gtm datacenter, glob, gtm datacenter, list, modify, regex, reset-stats, show, tmsh
Chapter 19

listener

Configures a Global Traffic Manager listener.

Module

gtm

Syntax

Configure the listener component within the gtm module using the following syntax.

Create/Modify

create listener [name]
modify listener [name]
options:
    address [ip address]
advertise [yes | no]
ip-protocol [tcp | udp]
pool [ [pool_name] | none]
profiles {
    [profile name]...
}
translate-address [enabled | disabled]
v1ans none
v1ans
[ add | delete | replace-all-with ] {
    [vlan name]...
}
v1ans-disabled
v1ans-enabled
edit listener { [ [name] | [glob] | [regex] ] ... }
options:
    all-properties
    non-default-properties
    one-line
reset-stats listener
reset-stats listener { [ [name] | [glob] | [regex] ] ... }
Display

list listener
list listener [ [ [name] | [glob] | [regex] ] ... ]
show running-config listener
show running-config listener [ [ [name] | [glob] | [regex] ] ... ]
  options:
    all-properties
    non-default-properties
    one-line
    partition
show listener
show listener [name]
  options:
    (default | gig | kil | meg | raw)
    field-fmt

Delete

  delete listener [name]

Description

You can use the listener component to create, display, modify, or delete a listener. A listener is an object that processes DNS queries. Listeners are defined for specific IP addresses and are always associated with port 53.

⚠️ Important

When you create, modify, or delete a listener, the system saves the running configuration in the stored configuration files.

Examples

Creates a listener named my_listener with an IP address of 10.10.1.1:
create listener my_listener address 10.10.1.1

Displays all non-default properties for all listeners:
list listener non-default-properties

Deletes the listener named my_listener:
delete listener my_listener
Options

You can use these options with the listener component:

- **address**
  Specifies the IP address on which the system listens. The system receives traffic sent to this IP address and processes it as needed. This option is required.

- **advertise**
  Specifies whether to advertise the listener address to surrounding routers. The options are yes or no. The default value is no.

- **glob**
  Displays the items that match the glob expression. For a description of glob expression syntax, see the glob man page.

- **ip-protocol**
  Specifies the protocol on which this listener receives network traffic. The options are udp or tcp. The default value is udp.

- **name**
  Specifies a unique name for the component. This option is required for the create and modify commands.

- **partition**
  Displays the administrative partition within which the listener resides.

- **pool**
  Specifies a default pool to which you want the listener to automatically direct traffic. The default value is none.

- **profiles**
  Specifies the DNS profile to use for this listener. Deleting a DNS profile from this listener will eliminate it from GTM's view. If none specified, then generic dns profile is added.

- **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. For a description of regular expression syntax, see the regex man page.

- **translate-regex**
  Enables or disables address translation for the listener. Disable address translation for a listener if you want to use the listener to load balance connections to any address. This option is useful when the system is load balancing devices that have the same IP address. The default value is disabled.

- **vlans**
  Specifies a list of VLANs on which traffic is either disabled or enabled, based on whether the vlans-disabled or vlans-enabled option is specified.

- **vlans-disabled**
  Specifies that traffic is not accepted by this listener on the VLANs specified in the vlans option. This option and the vlans-enabled option are mutually exclusive.
◆ vlans-enabled
Specifies that traffic is accepted by this listener on only the VLANS specified in the vlans option. This option and the vlans-disabled option are mutually exclusive.

See also

create, delete, edit, glob, list, modify, net vlan, net vlan-group, regex, reset-stats, show, tmsh
path

Displays or resets path statistics for the Global Traffic Manager.

Module

gtm

Syntax

Configure the path component within the gtm module using the following syntax.

Display

show path

options:
(default | exa | gig | kil | meg | peta | raw | tera | yotta | zetta)
field-fmt

Description

You can use the path component to display path statistics for the Global Traffic Manager. You can also reset the traffic statistics to zero (0) at any time.

Options

For more information about options for the show command, see show, on page 3-39.

See also

show, tmsh
**Persist**

Displays persistence records for the Global Traffic Manager.

**Module**

**gtm**

**Syntax**

Displays statistics for the **persist** component within the **gtm** module using the following syntax.

**Display**

```
show persist
```

**options:**

- **destination** [ [destination] | none]
- **ldns** [ip address]
- **level** [application | datacenter | link | pool-member | server | wideip]
- **max-results** [integer]
- **target-name** [ [name] | none]
- **target-type** [application | datacenter | link | pool-member | server | wideip]

**Description**

You can use the **persist** component to display various persistence records based on the filtering options that you use.

**Examples**

Displays all Global Traffic Manager persistence records:

```
show persist
```

Displays persistence records only for links:

```
show persist level link
```

**Options**

You can use these options with the **persist** component:

- **destination**
  
  Displays persistence records for the specified destination.
◆ ldns
   Displays persistence records for the specified LDNS address.

◆ level
   Displays persistence records for the specified level (destination type).

◆ max-results
   Specifies the maximum number of persistence records that you want the
   system to return.

◆ target-name
   Displays persistence records for the specified target.

◆ target-type
   Displays persistence records for the specified type of target.

See also

  show, tmsh
pool

Configures load balancing pools for the Global Traffic Manager.

Module

gtm

Syntax

Configure the Global Traffic Manager pool component within the gtm module using the following syntax.

Create/Modify

create pool [name]
modify pool [name]

options:
alternate-mode [drop-packet | fallback-ip | global-availability | none | \ packet-rate | ratio | return-to-dns | round-robin | static-persistence | topology | virtual-server-capacity | virtual-server-score]
canonical-name [name]
description [string]
[disabled | enabled]
dynamic ratio [disabled | enabled]
fallback-ipv4 [ip address]
fallback-ipv6 [ip address]
fallback-mode [completion-rate | cpu | drop-packet | fallback-ip | fewest-hops | \ global-availability | kilobytes-per-second | least-connections | \ lowest-round-trip-time | none | packet-rate | quality-of-service | ratio | \ return-to-dns | round-robin | static-persistence | topology | \ virtual-server-capacity | virtual-server-score]
limit-max-bps [integer]
limit-max-bps-status [disabled | enabled]
limit-max-connections [integer]
limit-max-connections-status [disabled | enabled]
limit-max-pps [integer]
limit-max-pps-status [disabled | enabled]
load-balancing-mode [completion-rate | cpu | drop-packet | fallback-ip | \ fewest-hops | global-availability | kilobytes-per-second | least-connections | \ lowest-round-trip-time | packet-rate | quality-of-service | ratio | \ return-to-dns | round-robin | static-persistence | topology | \ virtual-server-capacity | virtual-server-score]
manual-resume [disabled | enabled]
max-addresses-returned [integer]
members none
members
   [ add | delete | modify | replace-all-with ] {
      [vs-name] {
         options:
            depends-on none
            depends-on
               [ add | delete | replace-all-with ] {
                  [vs-name]...
               }
         [disabled | enabled]
         limit-max-bps [integer]
         limit-max-bps-status [disabled | enabled]
         limit-max-connections [integer]
         limit-max-connections-status [disabled | enabled]
         limit-max-pps [integer]
         limit-max-pps-status [disabled | enabled]
         load-balancing-mode
         monitor [disabled | enabled]
         order [integer]
         ratio
      }
   ...
}
metadata
   [add | delete | modify] {
      [metadata_name ... ] {
         value [ "value content" ]
         persist [ true | false ]
      }
   }
monitor [name]
qos-hit-ratio [integer]
qos-hops [integer]
qos-kilobytes-second [integer]
qos-lcs [integer]
qos-packet-rate [integer]
qos-rtt [integer]
qos-topology [integer]
qos-vs-capacity [integer]
qos-vs-score [integer]
ttl [integer]
verify-member-availability [disabled | enabled]
edit pool [ [ [name] | [glob] | [regex] ] ... ]
   options:
      all-properties
      non-default-properties
reset-stats pool
reset-stats pool [ [ [name] | [glob] | [regex] ] ... ]
Display

list pool
list pool [ [ [name] | [glob] | [regex] ] ... ]
show running-config pool
show running-config pool [ [ [name] | [glob] | [regex] ] ... ]
options:
  all-properties
  non-default-properties
  members vs-name
  one-line
  partition
show pool
show pool [name]
options:
  (default | gig | kil | meg | raw)
  detail
  field-fmt

Delete

delete pool [name]

◆ Note
You must remove all references to a pool before you can delete the pool.

Description

You can use the pool component to configure the pool definitions on the Global Traffic Manager. You use a pool to group member servers together to use a common load balancing algorithm.

◆ Important
The names of pools and pool members must be no more than 63 characters in length.

Examples

Creates a Global Traffic Manager pool named my_pool with two members myServer:myVs and 10.2.3.12, where both members use the Round Robin load balancing method, and the default HTTP monitor checks for member availability:

create pool my_pool members add { member myServer:myVs member 10.2.3.12:http } monitor all http
Deletes the pool `my_pool`:
```
delte pool my_pool
```
Displays statistics for all pools:
```
show pool
```
Displays the properties of pool `my_pool`:
```
list pool my_pool
```

## Options

You can use these options with the `pool` component:

- **alternate-mode**
  Specifies the load balancing mode that the system uses to load balance name resolution requests among the members of this pool, if the preferred method is unsuccessful in picking a pool. You set the preferred mode using the `load-balancing-mode` option. The default value is `round-robin`.

  The options are:
  
  - **drop-packet**
    Specifies that the Global Traffic Manager does nothing with the packet, and drops the request.
  
  - **fallback-ip**
    Specifies that the Global Traffic Manager returns the IP address that you specify as an answer to the query.
  
  - **global-availability**
    Specifies that the Global Traffic Manager distributes connection requests to virtual servers included in the pool in the order in which they are listed.
  
  - **none**
    Specifies that the system skips the alternate load balancing mode and immediately tries the load balancing mode specified in the `fallback-mode` option. If the value of the `fallback-mode` option is `none`, and you have multiple pools configured, the Global Traffic Manager uses the next available pool.
  
  - **packet-rate**
    Specifies that the Global Traffic Manager assigns connection requests to the virtual server that is currently processing the fewest number of packets per second.
  
  - **ratio**
    Specifies that the Global Traffic Manager distributes connection requests among a pool of virtual servers using a weighted Round Robin load balancing method.
  
  - **return-to-dns**
    Specifies that the Global Traffic Manager immediately returns connection requests to the local DNS for resolution.
• **round-robin**
  Specifies that the Global Traffic Manager distributes connection requests in a circular and sequential pattern among the virtual servers in a pool.

• **static-persistence**
  Specifies that the Global Traffic Manager consistently maps an LDNS IP address to the same available virtual server for the duration of a session.

• **topology**
  Specifies that the Global Traffic Manager uses proximity-based load balancing to distribute connection requests.

• **virtual-server-capacity**
  Specifies that the Global Traffic Manager distributes connection requests by creating a list of the virtual servers, weighted by capacity, then picks one of the virtual servers from the list. The virtual servers with the greatest capacity are picked most often, but over time all virtual servers are returned.

• **virtual-server-score**
  Specifies that the Global Traffic Manager assigns connection requests to virtual servers based on a user-defined ranking system.

◆ **canonical-name**
  Specifies the canonical name of the zone, for example, `www.siterequest.com`, that the system uses for CNAME dynamic delegation. The default value is **none**.

◆ **description**
  User-defined description.

◆ **[disabled | enabled]**
  Specifies whether this pool is available for load balancing. The default value is **enabled**.

◆ **dynamic-ratio**
  Enables or disables a dynamic ratio load balancing algorithm for this pool. This option is applicable only when you also configure the **load-balancing-mode** option for the pool with one of these dynamic load balancing modes:

  • **completion-rate**
  • **fewest-hops**
  • **kilobytes-per-second**
  • **least-connections**
  • **lowest-round-trip-times**
  • **quality-of-service**
  • **virtual-server-capacity**
  • **virtual-server-score**
When this option is **disabled** (the default), the system uses only the server or virtual server with the best metrics, or highest Quality of Service (QoS) score, for load balancing. When this option is **enabled**, the system treats QoS scores as ratios, and it uses each server or virtual server in proportion to the ratio determined by the QoS calculation.

- **fallback-ipv4**
  Specifies the IPv4 address of the server to which the system directs requests in the event that the load balancing methods configured for this pool fail to return a valid virtual server. Use this option for A-type DNS queries. The default value is `::`.

- **fallback-ipv6**
  Specifies the IPv6 address of the server to which the system directs requests in the event that the load balancing methods configured for this pool fail to return a valid virtual server. Use this option for AAAA- and A-type DNS queries. The default value is `::`.

- **fallback-mode**
  Specifies the load balancing mode that the system uses to load balance name resolution requests among the members of this pool, if the preferred and alternate modes are unsuccessful in picking a pool. You set the preferred mode using the **load-balancing-mode** option, and the alternate mode using the **alternate-mode** option. The default value is **return-to-dns**.

The options are:

- **completion-rate**
  Specifies that the Global Traffic Manager selects the virtual server that currently maintains the least number of dropped or timed-out packets during a transaction between a data center and the client LDNS.

- **cpu**
  Specifies that the Global Traffic Manager selects the virtual server that currently has the most CPU processing time available to handle name resolution requests.

- **drop-packet**
  Specifies that the Global Traffic Manager does nothing with the packet and drops the request.

- **fallback-ip**
  Specifies that the Global Traffic Manager returns the IP address that you specify as an answer to the query.

- **fewest-hops**
  Specifies that the Global Traffic Manager distributes connection requests to the virtual server in the data center that has the fewest router hops from the Local DNS.

- **global-availability**
  Specifies that the Global Traffic Manager distributes connection requests to virtual servers included in the pool in the order in which they are listed.
• **kilobytes-per-second**
  Specifies that the Global Traffic Manager distributes connection requests to the virtual server that is currently processing the fewest number of kilobytes per second.

• **least-connections**
  Specifies that the Global Traffic Manager distributes connection requests to the virtual server on Local Traffic Manager™ that currently hosts the fewest connections.

• **lowest-round-trip-time**
  Specifies that the Global Traffic Manager distributes connection requests to the virtual server with the fastest measured round trip time between a data center and a client LDNS.

• **none**
  Specifies that there is no fallback mode. If the system cannot use the preferred or alternate load balancing modes, it uses the next pool to resolve the request. If there are no more pools available, the result is the same as when the value for the `fallback-mode` option is `return-to-dns`.

• **packet-rate**
  Specifies that the Global Traffic Manager assigns connection requests to the virtual server that is currently processing the fewest number of packets per second.

• **quality-of-service**
  Specifies that the Global Traffic Manager distributes connection requests using current performance information to calculate an overall score for each virtual server, and then distributes connections to the virtual servers based on these scores.

• **ratio**
  Specifies that the Global Traffic Manager distributes connection requests among a pool of virtual servers using a weighted Round Robin load balancing method.

• **return-to-dns**
  Specifies that the Global Traffic Manager immediately returns connection requests to the local DNS for resolution.

• **round-robin**
  Specifies that the Global Traffic Manager distributes connection requests in a circular and sequential pattern among the virtual servers in a pool.

• **static-persistence**
  Specifies that the Global Traffic Manager consistently maps an LDNS IP address to the same available virtual server for the duration of a session.

• **topology**
  Specifies that the Global Traffic Manager distributes connection requests using proximity-based load balancing.

• **virtual-server-capacity**
  Specifies that the Global Traffic Manager distributes connection requests by creating a list of the virtual servers, weighted by capacity,
then picks one of the virtual servers from the list. The virtual servers with the greatest capacity are picked most often, but over time all virtual servers are returned.

- **virtual-server-score**
  Specifies that the Global Traffic Manager distributes connection requests to virtual servers based on a user-defined ranking system.

- **glob**
  Displays the items that match the glob expression. For a description of glob expression syntax, see the glob man page.

- **limit-max-bps**
  Specifies the maximum allowable data throughput rate, in bits per second, for the virtual servers in the pool. If the network traffic volume exceeds this value, the system marks the pool as unavailable. The default value is 0 (zero).

- **limit-max-bps-status**
  Enables or disables the limit-max-bps option for this pool. The default value is disabled.

- **limit-max-connections**
  Specifies the number of current connections allowed for the virtual servers in the pool. If the current connections exceed this value, the system marks the pool as unavailable. The default value is 0 (zero).

- **limit-max-connections-status**
  Enables or disables the limit-max-connections option for this pool. The default value is disabled.

- **limit-max-pps**
  Specifies the maximum allowable data transfer rate, in packets per second, for the virtual servers in the pool. If the network traffic volume exceeds this value, the system marks the pool as unavailable. The default value is 0 (zero).

- **limit-max-pps-status**
  Enables or disables the limit-max-pps option for this pool. The default value is disabled.

- **load-balancing-mode**
  Specifies the preferred load balancing mode that the system uses to load balance name resolution requests among the members of this pool. The default value is round-robin.

The options are:

- **completion-rate**
  Specifies that the Global Traffic Manager selects the virtual server that currently maintains the least number of dropped or timed-out packets during a transaction between a data center and the client LDNS.

- **cpu**
  Specifies that the Global Traffic Manager selects the virtual server that currently has the most CPU processing time available to handle name resolution requests.
• **drop-packet**  
  Specifies that the Global Traffic Manager does nothing with the packet and drops the request.

• **fallback-ip**  
  Specifies that the Global Traffic Manager returns the IP address that you specify as an answer to the query.

• **fewest-hops**  
  Specifies that the Global Traffic Manager distributes connection requests to the virtual server in the data center that has the fewest router hops from the Local DNS.

• **global-availability**  
  Specifies that the Global Traffic Manager distributes connection requests to virtual servers included in the pool in the order in which they are listed.

• **kilobytes-per-second**  
  Specifies that the Global Traffic Manager distributes connection requests to the virtual server that is currently processing the fewest number of kilobytes per second.

• **least-connections**  
  Specifies that the Global Traffic Manager distributes connection requests to the virtual server on Local Traffic Manager that currently hosts the fewest connections.

• **lowest-round-trip-time**  
  Specifies that the Global Traffic Manager distributes connection requests to the virtual server with the fastest measured round trip time between a data center and a client LDNS.

• **packet-rate**  
  Specifies that the Global Traffic Manager assigns connection requests to the virtual server that is currently processing the fewest number of packets per second.

• **quality-of-service**  
  Specifies that the Global Traffic Manager distributes connection requests using current performance information to calculate an overall score for each virtual server, and then distributes connections to the virtual servers based on these scores.

• **ratio**  
  Specifies that the Global Traffic Manager distributes connection requests among a pool of virtual servers using a weighted Round Robin load balancing method.

• **return-to-dns**  
  Specifies that the Global Traffic Manager immediately returns connection requests to the local DNS for resolution.

• **round-robin**  
  Specifies that the Global Traffic Manager distributes connection requests in a circular and sequential pattern among the virtual servers in a pool.
• **static-persistence**
  Specifies that the Global Traffic Manager consistently maps an LDNS IP address to the same available virtual server for the duration of a session.

• **topology**
  Specifies that the Global Traffic Manager distributes connection requests using proximity-based load balancing.

• **virtual-server-capacity**
  Specifies that the Global Traffic Manager distributes connection requests by creating a list of the virtual servers, weighted by capacity, then picks one of the virtual servers from the list. The virtual servers with the greatest capacity are picked most often, but over time all virtual servers are returned.

• **virtual-server-score**
  Specifies that the Global Traffic Manager distributes connection requests to virtual servers based on a user-defined ranking system.

◆ **manual-resume**
  Enables or disables the manual resume function for this pool. If you leave this option disabled (the default), then a member of this pool automatically becomes available for load balancing when its status changes from down to up. When the manual-resume option is enabled, if the status of a member of this pool changes from up to down, the pool member remains disabled indefinitely, until you manually re-enable it.

◆ **max-address-returned**
  Specifies the maximum number of available virtual servers that the system lists in an A record response. The default value is 1.

◆ **members**
  Specifies the IP address and port number of the pool members. The default value is none. You can also use the following option with pool members:

  • **depends-on**
    Specifies the name of the virtual server on which this pool member depends.

◆ **description**
  User-defined description.

• **[enabled | disabled]**
  Specifies whether this pool member is available for load balancing. The default value is enabled.

• **limit-max-bps**
  Specifies the maximum allowable data throughput rate, in bits per second, for the pool member. If the network traffic volume exceeds this value, the system marks the pool member as unavailable.

• **limit-max-bps-status**
  Enables or disables the limit-max-bps option for this pool member. The default value is disabled.
- **limit-max-connections**
  Specifies the number of current connections allowed for this pool member. If the current connections exceed this value, the system marks this pool member as unavailable.

- **limit-max-connections-status**
  Enables or disables the limit-max-connection option for this pool member. The default value is disabled.

- **limit-max-pps**
  Specifies the maximum allowable data transfer rate, in packets per second, for this pool member. If the network traffic volume exceeds this value, the system marks this pool member as unavailable.

- **limit-max-pps-status**
  Enables or disables the limit-max-pps option for this pool member. The default value is disabled.

- **monitor**
  Enables or disables the monitor assigned to this pool member. The default value is enabled.

- **order**
  Specifies the order number of the pool member. The system uses this number with load balancing methods that involve prioritizing pool members, such as the Ratio load balancing method.

- **ratio**
  Specifies the weight of the pool member for load balancing purposes.

- **vs-name**
  Displays the name of the corresponding virtual server.

- **metadata**
  Specifies user-defined data to associate with a server. By default the persist attribute is set to true. This means the data is saved into the configuration file.

- **monitor**
  Specifies the health monitors that the system uses to determine whether it can use this pool for load balancing. The default value is none.

- **name**
  Specifies a unique name for the component. This option is required for the create and modify commands.

- **partition**
  Displays the administrative partition within which the component resides.

- **qos-hit-ratio**
  Assigns a weight to the Hit Ratio performance factor when the value of the either the load-balancing-mode or fallback-mode options is quality-of-service. The default value is 5.

- **qos-hops**
  Assigns a weight to the Hops performance factor when the value of the either the load-balancing-mode or fallback-mode options is quality-of-service. The default value is 0 (zero).
◆ qos-kilobytes-second
Assigns a weight to the Kilobytes per Second performance factor when the value of the either the load-balancing-mode or fallback-mode options is quality-of-service. The default value is 3.

◆ qos-lcs
Assigns a weight to the Link Capacity performance factor when the value of the either the load-balancing-mode or fallback-mode options is quality-of-service. The default value is 30.

◆ qos-packet-rate
Assigns a weight to the Packet Rate performance factor when the value of the either the load-balancing-mode or fallback-mode options is quality-of-service. The default value is 1.

◆ qos-rtt
Assigns a weight to the Round Trip Time performance factor when the value of the either the load-balancing-mode or fallback-mode options is quality-of-service. The default value is 50.

◆ qos-topology
Assigns a weight to the Topology performance factor when the value of the either the load-balancing-mode or fallback-mode options is quality-of-service. The default value is 0 (zero).

◆ qos-vs-capacity
Assigns a weight to the Virtual Server performance factor when the value of the either the load-balancing-mode or fallback-mode options is quality-of-service. The default value is 0 (zero).

◆ qos-vs-score
Assigns a weight to the Virtual Server Score performance factor when the value of the either the load-balancing-mode or fallback-mode options is quality-of-service. The default value is 0 (zero).

◆ regex
Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. For a description of regular expression syntax, see the regex man page.

◆ ttl
Specifies the amount of time, in d:h:m:s, h:m:s, m:s, or seconds, that the IP address, once found, is valid. Once the time-to-live (TTL) expires, the client has to request the IP address resolution again. The valid values are 0 through 4294967295; the default value is 30.

◆ verify-member-availability
Specifies that the system verifies the availability of the members before sending a connection to those resources. The default value is enabled.

See also
cli admin-partitions, create, delete, edit, glob, gtm monitor, list, ltm default-node-monitor, ltm virtual, modify, regex, reset-stats, show, tmsh
prober-pool

Configures prober pools for the Global Traffic Manager.

Module

gtm

Syntax

Configure the Global Traffic Manager prober-pool component within the gtm module using the following syntax.

Create/Modify

create prober-pool [name]
modify prober-pool [name]

options:
  description [string]
  [disabled | enabled]
  load-balancing-mode [global-availability | round-robin]
  members none

members
  [ add | delete | modify | replace-all-with ] {
    [name] {
      options:
        description [string]
        [disabled | enabled]
        order [integer]
    }...
  }

edit prober-pool [ [ [name] | [glob] | [regex] ] ... ]

options:
  all-properties
  non-default-properties

reset-stats prober-pool
reset-stats prober-pool [ [ [name] | [glob] | [regex] ] ... ]

Display

list prober-pool
list prober-pool [ [ [name] | [glob] | [regex] ] ... ]

show running-config prober-pool
show running-config prober-pool [ [ [name] | [glob] | [regex] ] ... ]
Chapter 19

options:
  all-properties
  non-default-properties
show prober-pool
show prober-pool [name]
  options:
    (default | exa | gig | kil | meg | peta | raw | tera | yotta | zetta)
  detail
  field-fmt

Delete

dele prober-pool [name]

◆ Note
You must remove all references to a pool before you can delete the pool.

Description

You can use the prober-pool component to configure prober pool definitions on the Global Traffic Manager. You use prober pools to control which BIG-IP servers on your network are utilized by GTM to monitor the up/down state of GTM resources. Once defined, prober pools can be set to monitor whole data centers or individual servers.

◆ Note
You must remove all references to a prober-pool before you can delete the prober-pool.

Examples

Creates a Global Traffic Manager prober pool with two members bigip-dallas and bigip-london. Members are selected using the global-availability load balancing method:

create prober-pool my_pool members add { bigip-dallas bigip-london }

Deletes the prober pool my_pool:

delete prober-pool my_pool

Displays statistics for all prober pools:

show prober-pool

Displays settings of prober pool my_pool:

list prober-pool my_pool
Options

You can use these options with the **prober-pool** component:

- **description**
  User-defined description.

- **glob**
  Displays the items that match the **glob** expression. See **help glob** for a description of **glob** expression syntax.

- **load-balancing-mode**
  Specifies the load balancing mode that the system uses to select members of this pool. The default value is **global-availability**.
  The options are:
  - **global-availability**
    Specifies that the Global Traffic Manager selects the first available pool member in the order in which they are listed.
  - **round-robin**
    Specifies that the Global Traffic Manager selects members using a circular, sequential pattern among available pool members.

- **members**
  Specifies the BIG-IP server names of the pool members. The default value is **none**. You can also use the following options with prober pool members:
  - **description**
    User-defined description.
  - **enabled | disabled**
    Specifies whether this pool member is available to issue probes. The default value is **enabled**.
  - **order**
    Specifies the order number of the pool member. The system uses this number with load balancing methods that involve prioritizing pool members by listed order.

- **name**
  Specifies a unique name for the component. This option is required for the commands **create**, **delete**, and **modify**.

- **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. See **help regex** for a description of regular expression syntax.

See also

region

Configures a Global Traffic Manager region.

Module

gtm

Syntax

Configure the region component within the gtm module using the following syntax.

Create/Modify

create region [name]
modify region [name]
  options:
    description [string]
    region-members
      options:
        continent [Africa | Antartica | Asia | Australia | Europe | North America | South America | unknown]
        country [two-letter abbreviation of country name]
        datacenter [name]
        isp [AOL | BeijingCNC | CNC | ChinaTelecom | Comcast | Earthlink | ShanghaiCNC | ShanghaiTelecom]
        not [continent | country | datacenter | isp | pool | region-name | subnet]
        pool [name]
        region-name [name]
        state [name]
    subnet

edit region [ [ [name] | [glob] | [regex] ] ... ]
  options:
    all-properties

Display

list region
list region [ [ [name] | [glob] | [regex] ] ... ]
show running-config region
show running-config region [ [ [name] | [glob] | [regex] ] ... ]
options:
   all-properties
   one-line

Delete

delete region [name]

Description

You can use the region component to create, display, modify, or delete a region. A region is a customized collection of topologies with which you can extend the topology functionality by defining specific geographical regions that have meaning for your network.

Examples

Creates a region named my_region to populate with resources on the continent of Australia:

create region my_region continent Australia

Displays properties for all regions:

list region

Deletes the region named my_region:

delete region my_region

Options

You can use these options with the region component:

- **description**
  User-defined description.

- **glob**
  Displays the items that match the glob expression. For a description of glob expression syntax, see the glob man page.

- **name**
  Specifies a unique name for the component. This option is required for the create and modify commands.

- **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. For a description of regular expression syntax, see the regex man page.
◆ **region-members**
   Specifies the members that you want to add to, delete from, replace-all-with, or modify for this region. You can specify the following options for region members:
   - **continent**
     The name of a continent.
   - **country**
     The two-letter abbreviation of a country. Use the command completion feature to view the numerous options.
   - **datacenter**
     The name of an existing data center.
   - **isp**
     The name of an internet service provider.
   - **not**
     Region-members to exclude from this region.
   - **pool**
     The name of an existing pool.
   - **region-name**
     The name of an existing region.
   - **state**
     Specifies the name of an existing state.
   - **subnet**
     An existing subnet.

**See also**

create, delete, edit, glob, list, modify, regex, show, tmsh
rule

Opens an editor in which you can configure iRules® for traffic management system configuration.

Module

gtm

Syntax

Configure the rule component within the gtm module using the following syntax.

Create/Modify

create rule [name]
modify rule [name]

option:

metadata

[add | delete | modify] {
[metadata_name] {
value [ "value content" ]
persist [ true | false ]
}
}

edit rule [ [ [name] | [glob] | [regex] ] ... ]

Display

list rule
list rule [ [ [name] | [glob] | [regex] ] ... ]
show running-config rule
show running-config rule [ [ [name] | [glob] | [regex] ] ... ]

options:

all-properties
non-default-properties
show rule
show rule [ [ [name] | [glob] | [regex] ] ... ]

options:

(default | exa | gig | kil | meg | peta | raw | tera | yotta | zetta)
Delete

delete rule [name]

◆ Note

You can also delete meta data associated with an iRule. See the example section for more information.

Description

You can use iRules to direct traffic not only to specific pools, but also to individual pool members, including port numbers and URI paths, either to implement persistence or to meet specific load balancing requirements. The syntax that you use to write iRules is based on the Tools Command Language (Tcl) programming standard. Thus, you can use many of the standard Tcl commands, plus a robust set of extensions that the BIG-IP Local Traffic Manager system provides to help you further increase load balancing efficiency.

For information about standard Tcl syntax, see http://tmml.sourceforge.net/doc/tcl/index.html. For a list of Tcl commands that have been disabled within the traffic management system and therefore cannot be used in the traffic management system, see the Configuration Guide for BIG-IP Local Traffic Manager™. This guide is available at http://support.f5.com.

Examples

Opens the vi editor in which you can edit the iRule named my_irule. After you close the editor, you must type the command sequence save config to save the configuration changes to the stored configuration files:

```
edit rule my_irule
```

The following are example iRules for the Global Traffic Manager:

Specifies that requests from 10.10.1.0/24 be directed to cname.siterequest.com, and that all other requests be directed to 10.20.20.20:

```
when DNS_REQUEST {
    if { [IP::addr [IP::remote_addr]/24 equals 10.10.1.0/24] } {
        (cname cname.siterequest.com ) else { host 10.20.20.20} }
```

Specifies that requests that originate in Asia be directed to the pool named asia_pool, and that all other requests be directed to the pool named general_pool:

```
when DNS_REQUEST {
    if { [whereis [IP::remote_addr] ] contains "Asia"} {
        (pool asia_pool) else {pool general_pool} }
```
Adds new metadata to named `my_meta` and modifies existing metadata named `my_meta2` for the iRule named `my_irule`.

```bash
modify rule my_irule {
    when DNS_REQUEST {} 
    metadata replace-all-with {
        my_meta {
            persist false
            value "hello"
        }
        my_meta2 {
            persist false
            value "hello 2"
        }
    }
}
```

Deletes metadata named `my_meta` from the iRule named `my_irule`.

```bash
modify rule my_irule {
    when RULE_INIT {} 
    definition-checksum 7c0dba9aa53e8959042c6cfe041d3d11
    metadata delete { my_meta }
}
```

### Options

You can use the following options with the `rule` component:

- **glob**
  Displays the items that match the `glob` expression. For a description of `glob` expression syntax, see the `glob` man page.

- **metadata**
  Specifies a user-defined key/value pair.

- **name**
  Specifies a unique name for the component. This option is required.

- **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. For a description of regular expression syntax, see the `regex` man page.

### See also

`edit`, `glob`, `list`, `regex`, `show`, `tmsh`
**server**

Configures servers for the Global Traffic Manager.

**Module**

`gtm`

**Syntax**

Configure the `server` component within the `gtm` module using the following syntax.

**Create/Modify**

```
create server [name]
modify server [name]
```

options:
- `addresses none`
- `addresses`

```
 [add | delete | replace-all-with] {
 [ip address] {
  [unit-id [integer] ]
  [translation [ip address] ]
  [explicit-link-name [name] ]
 }
}
datacenter
datacenter [name]
description [string]
[disabled | enabled]
expose-route-domains [no | yes]
iq-allow-path [no | yes]
iq-allow-service-check [no | yes]
iq-allow-snmp [no | yes]
limit-cpu-usage [integer]
limit-cpu-usage-status [disabled | enabled]
limit-bps [integer]
limit-bps-status [disabled | enabled]
limit-connections [integer]
limit-connections-status [disabled | enabled]
limit-pps [integer]
limit-pps-status [disabled | enabled]```
limit-mem-avail [integer]
limit-mem-avail-status [disabled | enabled]
link-discovery [disabled | enabled]
metadata
   [add | delete | modify] {
       [metadata_name ...] {
           value "value content"
           persist [true | false]
       }
   }

monitor [none | [name]]
prober-pool [none | name]
product [name]
virtual-server-discovery [disabled | enabled]
virtual-servers none
virtual-servers
   [add | delete | replace-all-with] {
       [vs-name] {
           options:
           depends-on none
           depends-on
           [add | delete | replace-all-with] {
               [server_name:vs-name] ...
           }
           description [string]
           destination [ipv4_address:port | ipv6_address:port]
           [disabled | enabled]
           explicit-link-name [none | [name]]
           limit-max-bps [integer]
           limit-max-bps-status [disabled | enabled]
           limit-max-connections [integer]
           limit-max-connections-status [disabled | enabled]
           limit-max-pps [integer]
           limit-max-pps-status [disabled | enabled]
           monitor [name]
           translation-address [ip address]
           translation-port [integer | [name]]
       }
   }

edit server ...]
   options:
   all-properties
   non-default-properties
   one-line
reset-stats server
reset-stats server [ [ name ] | [ glob ] | [ regex ] ] ...

Display

list server
list server [ [ name ] | [ glob ] | [ regex ] ] ...
show running-config server
show running-config server [ [ name ] | [ glob ] | [ regex ] ] ...
options:
  all-properties
  non-default-properties
  one-line
  partition
show server
show server [ [ name ] | [ glob ] | [ regex ] ] ...
options:
  (default | gig | kil | meg | raw)
  detail
  field-fmt

Delete

delete server [name]

Description

You can use the server component to configure a Global Traffic Manager server.

Important
The name of a server must be no more than 63 characters in length.

Examples

Creates a server named my_server in my_datacenter with a self IP address of 10.10.1.1:

create server my_server addresses add {10.10.1.1} datacenter my_datacenter

Adds the virtual server myVs with an IP address of 10.10.10.2:80 as a resource to the server named my_server:

modify server my_server virtual-servers add {myVs { address 10.10.10.2:80 } }

Displays all non-default properties for all servers:

list server non-default-properties
Deletes the server named `my_server`:
```
delete server my_server
```

## Options

You can use these options with the `server` component:

- **addresses**
  Specifies the self IP addresses for the server. This option is required for the `create` command.

  You can also specify the following options.

  - **translation**
    Specifies the internal IP address that corresponds to the external IP address of this server. The default value is `::`.

  - **unit-id**
    Specifies the unit ID number for this server in a redundant system. The default value is **1**.

- **description**
  User-defined description.

- **datacenter**
  Specifies the data center to which the server belongs. This option is required for the `create` command.

- **[disabled | enabled]**
  Enables or disables the server. The default value is **enabled**.

- **expose-route-domains**
  Allow the GTM server to auto-discover LTM virtual servers from all route domains. The default value is **no**.

- **glob**
  Displays the items that match the `glob` expression. For a description of `glob` expression syntax, see the `glob` man page.

- **iq-allow-path**
  Specifies whether the Global Traffic Manager uses this BIG-IP system to conduct a path probe before delegating traffic to it. The default value is **yes**.

- **iq-allow-service-check**
  Specifies whether the Global Traffic Manager uses this BIG-IP system to conduct a service check probe before delegating traffic to it. The default value is **yes**.

- **iq-allow-snmp**
  Specifies whether the Global Traffic Manager uses this BIG-IP system to conduct an SNMP probe before delegating traffic to it. The default value is **yes**.

- **limit-cpu-usage**
  For a server configured as a generic host, specifies the percent of CPU usage; otherwise has no effect. If percent of CPU usage goes above the limit, the system marks the server as unavailable.
◆ limit-cpu-usage-status
Enables or disables the limit-cpu-usage option for this server. Only has an effect on a server configured as a generic host. The default value is disabled.

◆ limit-max-bps
Specifies the maximum allowable data throughput rate, in bits per second, for this server. If the network traffic volume exceeds this limit, the system marks the server as unavailable.

◆ limit-max-bps-status
Enables or disables the limit-max-bps option for this server. The default value is disabled.

◆ limit-max-connections
Specifies the maximum number of concurrent connections, combined, for this server. If the connections exceed this limit, the system marks the server as unavailable.

◆ limit-max-connections-status
Enables or disables the limit-max-connections option for this server. The default value is disabled.

◆ limit-max-pps
Specifies the maximum allowable data transfer rate, in packets per second, for this server. If the network traffic volume exceeds this limit, the system marks the server as unavailable.

◆ limit-max-pps-status
Enables or disables the limit-max-pps option for this server. The default value is disabled.

◆ limit-mem-avail
For a server configured as a generic host, specifies the available memory required by the virtual servers on the server. If available memory falls below this limit, the system marks the server as unavailable.

◆ limit-mem-avail-status
Enables or disables the limit-mem-avail option for this server. Only used on a server configured as a generic host. The default value is disabled.

◆ link-discovery
Specifies whether the system auto-discovers the links for this server. The default value is disabled.

The options are:
• disabled
  Specifies that the system does not auto-discover the links that are available for the server.
• enabled
  Specifies that the system auto-discovers the links that are configured on the server. With this option, the system automatically adds, deletes, and modifies link settings in the configuration.
• enabled-no-delete
  Specifies that the system auto-discovers the links that are configured on the server. With this option, the system automatically adds and
modifies link settings in the configuration, but does not delete them. This option is useful when you regularly take links in and out of service.

- **metadata**
  Specifies user-defined data to associate with a server. By default the `persist` attribute is set to `true`. This means the data is saved into the configuration file.

- **monitor**
  Specifies the health monitors that the system uses to determine whether this server is available for load balancing.

- **name**
  Specifies a unique name for the component. This option is required for the `create` and `modify` commands.

- **partition**
  Displays the administrative partition within which the object resides.

- **prober-pool**
  Specifies the name of a prober pool to use to monitor this server's resources. If this value is specified, it overrides any prober pool set on this server's data center. The default value is `none`.

- **product**
  Specifies the server type. The server type determines the metrics that the system can collect from the server. Use the command completion feature to view the types of servers that are available.

- **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (`@[regular expression]`) to indicate that the identifier is a regular expression. For a description of regular expression syntax, see the `regex` man page.

- **virtual-server-discovery**
  Specifies whether the system auto-discovers the virtual servers for this server. The default value is `disabled`.
  The options are:
  - **disabled**
    Specifies that the system does not auto-discover the virtual servers that are configured on the server. With this option, you must configure the virtual servers for this server.
  - **enabled**
    Specifies that the system auto-discovers the virtual servers that are configured on the server. With this option, the system automatically adds, deletes, and modifies virtual server settings in the configuration.
  - **enabled-no-delete**
    Specifies that the system auto-discovers the virtual servers that are configured on the server. With this option, the system automatically adds and modifies virtual server settings in the configuration, but does not delete them. This option is useful when you regularly take virtual servers in and out of service.
virtual-servers
Specifies the name of the virtual servers that are resources for this server. You can include the following options for virtual servers.

- **depends-on**
  Specifies the vs-name of the server on which this virtual server depends.

- **description**
  User-defined description.

- **destination**
  Specifies the IP address and port of the virtual server.

- **[disabled | enabled]**
  Specifies whether this virtual server is available for load balancing. The default value is **enabled**.

- **explicit-link-name**
  Specifies the explicit link name for the virtual server. The default value is **none**.

- **limit-max-bps**
  Specifies the maximum allowable data throughput rate, in bits per second, for this virtual server. If the network traffic volume exceeds this value, the system marks the virtual server as unavailable. The default value is **0** (zero).

- **limit-max-bps-status**
  Enables or disables the **limit-max-bps** option for this virtual server. The default value is **disabled**.

- **limit-max-connections**
  Specifies the number of current connections allowed for this virtual server. If the current connections exceed this value, the system marks this virtual server as unavailable. The default value is **0** (zero).

- **limit-max-connections-status**
  Enables or disables the **limit-max-connections** option for this virtual server. The default value is **disabled**.

- **limit-max-pps**
  Specifies the maximum allowable data transfer rate, in packets per second, for this virtual server. If the network traffic volume exceeds this limit, the system marks the virtual server as unavailable. The default value is **0** (zero).

- **limit-max-pps-status**
  Enables or disables the **limit-max-pps** option for this virtual server. The default value is **disabled**.

- **monitor**
  Specifies the monitor you want to assign to this virtual server. The default value is **none**.

- **translation-address**
  Specifies the public address that this virtual server translates into when the Global Traffic Manager communicates between the network and the Internet. The default value is **::**.
- **translation-port**
  Specifies the translation port number or service name for the virtual server, if necessary. The default value is 0.

See also

create, delete, edit, glob, gtm datacenter, gtm link, gtm prober-pool, list, modify, regex, reset-stats, show, tmsh
topology

Configures a topology statement.

Module

gtm

Syntax

Configure the topology component within the gtm module using the following syntax.

Create

create topology
    options:
        description [string]
        ldns: [continent | country | isp | not | region-name | state | subnet]
        server: [continent | country | datacenter | isp | not | pool |
            region-name | state | subnet]
        score [integer]
edit topology [ [name] | [glob] | [regex] ] ...
    options:
        all-properties
        non-default-properties

Display

list topology
list topology [ [name] | [glob] | [regex] ] ...
show running-config topology
show running-config topology [ [name] | [glob] | [regex] ] ...
    options:
        all-properties
        non-default-properties
        one-line

Delete

delete topology all
delete topology [ldns: [identifier] [value] server: [identifier] [value] ]
Description

You can use the `topology` component to configure a topology statement. A topology statement is a set of characteristics that identify the origin of a given name resolution request.

Examples

Creates a topology statement that specifies that the Global Traffic Manager routes any traffic coming from the United States to the datacenter named DC1. The weight of this topology item for load balancing is 30.
```
create topology ldns: country US server: datacenter DC1 score 30
```

Deletes the topology statement mentioned in the previous example:
```
delete topology ldns: country US server: datacenter DC1
```

Options

You can use the following options with the `topology` component:

- **description**
  User-defined description.

- **glob**
  Displays the items that match the `glob` expression. For a description of `glob` expression syntax, see the `glob` man page.

- **ldns:**
  Specifies the criteria that the Global Traffic Manager uses when matching requests from LDNS servers.
  - **continent**
    A continent whose IP address allocation range should be used in matching topologies.
  - **country**
    A country whose IP address allocation range should be used in matching topologies.
  - **datacenter**
    A data center to be used in matching topologies.
  - **isp**
    An ISP whose IP address allocation range should be used in matching topologies.
  - **not**
    Specify a region member to exclude from the region.
  - **pool**
    A pool to be used in matching topologies.
  - **region**
    Another region to be used in matching topologies.
• state
  A state whose IP address allocation range should be used in matching topologies.

• subnet
  A subnet to be used in matching topologies.

◆ regex
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. For a description of regular expression syntax, see the regex man page.

◆ score
  Specifies the weight of the topology item.

◆ server:
  Specifies the server to which the Global Traffic Manager routes requests.

  • continent
    A continent whose IP address allocation range should be used as an LDNS routing destination.

  • country
    A country whose IP address allocation range should be used as an LDNS routing destination.

  • datacenter
    A data center to be used as an LDNS routing destination.

  • isp
    An ISP whose IP address allocation range should be used as an LDNS routing destination.

  • not
    Specify a region member to exclude from the group.

  • pool
    A pool to be used as an LDNS routing destination.

  • region
    Another region to be used as an LDNS routing destination.

  • state
    A state whose IP address allocation range should be used as an LDNS routing destination.

  • subnet
    A subnet to be used as an LDNS routing destination.

See also

create, delete, edit, glob, gtm server, list, regex, show, tmsh
traffic

Displays traffic statistics for the Global Traffic Manager.

Module

gtm

Syntax

Configure the traffic component within the gtm module using the following syntax.

Display

show traffic

options:
(default | exa | gig | kil | meg | peta | raw | tera | yotta | zetta)

field-fmt

Description

You can use the traffic component to display global traffic statistics, including those for IPv4 and IPv6 requests, current Local Domain Name System (LDNS) servers, and current paths.

Options

For more information about options for the show command, see show, on page 3-39.

See also

show, sys tmm-traffic, tmsh
wideip

Configures a wide IP.

Module
gtm

Syntax

Configure the *wideip* component within the *gtm* module using the syntax shown in the following sections.

Create/Modify

```yaml
create wideip [name]
modify wideip [name]
```

options:

- aliases [name...name]
- description [string]
- [disabled | enabled]
- ipv6-no-error-neg-ttl [integer]
- ipv6-no-error-response [disabled | enabled]
- last-resort-pool [name]
- metadata
  - [add | delete | modify] {
    - [metadata_name ...] {
      - value ["value content"]
      - persist [true | false]
    }
  }
- [disabled | enabled]
- persist-cidr-ipv4 [integer]
- persist-cidr-ipv6 [integer]
- pool-lb-mode [name]
- pools none
- pools
  - [add | delete | modify | replace-all-with] {
    - [pool name]...
  }
- rules none
- rules
  - [add | delete | modify | replace-all-with] {
    - [rule name]...
  }
- ttl-persistence [integer]

```
edit wideip [ [name] | [glob] | [regex] ] ...
```

options:

- all-properties
- non-default-properties

reset-stats wideip

reset-stats wideip [ [name] | [glob] | [regex] ] ...
```
Display

```
list wideip [ [name] | [glob] | [regex] ] ... ]
show running-config wideip
show running-config wideip [ [name] | [glob] | [regex] ] ... ]
  options:
    all-properties
    non-default-properties
    one-line
    partition
show wideip
show wideip [ [ [name] | [glob] | [regex] ] ... ]
  options:
    (default | exa | gig | kil | meg | peta | raw | tera | yotta | zetta)
    (detail | global)
    field-fmt
```

Delete

```
delete wideip [all | [name] ]
```

Description

You can use the `wideip` component to create, modify, display, or delete a wide IP. A wide IP is a mapping of a fully-qualified domain name (FQDN) to a set of virtual servers that host the domain’s content, such as a web site or an e-commerce site.

Examples

```mayı
create wideip www.my_wide_ip.com
delete wideip www.my_wide_ip.com
Deletes the wide IP named www.my_wide_ip.
```

Options

- **aliases**
  Specifies alternate domain names for the Web site content you are load balancing. You can use two different wildcard characters, asterisk (*) and question mark (?), to represent one or more characters. The default value is none.

- **description**
  User defined description.

- **[disabled | enabled]**
  Specifies whether the wide IP and its resources are available for load balancing.
◆ **glob**
   Displays the items that match the `glob` expression. See `help glob` for a description of `glob` expression syntax.

◆ **ipv6-no-error-neg-ttl**
   Specifies the negative caching TTL of the SOA for the IPv6 NoError response. The default is 0, meaning no SOA is included (i.e. no caching).

◆ **ipv6-no-error-response**
   When **enabled**, specifies that the system returns a NoError response to IPv6 wide IP requests. This response is an authoritative empty answer from the system to AAAA record requests. With this option **enabled**, the system responds faster to IPv6 requests for which it does not have AAAA records configured. The default value is **disabled**.

◆ **last-resort-pool**
   Specifies which pool for the system to use as the last resort pool when load balancing requests for this wide IP. The default value is **none**.

◆ **metadata**
   Specifies user-defined data to associate with a server. By default the **persist** attribute is set to true. This means the data is saved into the configuration file.

◆ **name**
   Specifies a unique name for the component. This option is required for the commands **create** and **modify**.

◆ **partition**
   Displays the administrative partition within which the component resides.

◆ **persistence**
   When **enabled**, specifies that when a local DNS server makes repetitive requests on behalf of a client, the system reconnects the client to the same resource as previous requests. The default value is **disabled**.

◆ **persist-cidr-ipv4**
   Specifies a mask used to group IPv4 LDNS addresses. This feature allows one persistence record to be shared by LDNS addresses that match within this mask.

◆ **persist-cidr-ipv6**
   Specifies a mask used to group IPv6 LDNS addresses. This feature allows one persistence record to be shared by LDNS addresses that match within this mask.

◆ **pools**
   Configures the pools the system uses when load balancing requests for this wide IP. The default value is **none**.

◆ **pool-lb-mode**
   Specifies the load balancing method used to select a pool in this wide IP. This option is relevant only when multiple pools are configured for this wide IP. The default value is **round-robin**.

The available load balancing methods are:
• **global-availability**
  Specifies that the system selects a pool by following the order of the Pool list. The system repeatedly selects the first pool in the list for as long as its status is available. If the pool becomes unavailable for any reason, the system then repeatedly selects the next pool in the list, and so on.

• **random**
  Specifies that the system selects a pool in no pattern or order.

• **ratio**
  Specifies that the system selects a pool based on the ratio that you assign to the pool.

• **round-robin**
  Specifies that the system selects pools sequentially.

• **topology**
  Specifies that the system selects a pool based on topology information in the incoming LDNS request. Note that this load balancing method works only if you have configured a topology statement.

◆ **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. See help regex for a description of regular expression syntax.

◆ **rules**
  Specifies the iRules™ that this wide IP uses for load balancing decisions. The system evaluates the iRules in the order in which they are listed, until it finds a matching iRule. The default value is none.

◆ **ttl-persistence**
  Specifies, in seconds, the length of time for which a persistence entry is valid. This value can range from 0 through 2147483648 seconds. The default value is 3600.

See Also

create, delete, edit, glob, gtm pool, list, modify, regex, reset-stats, show, tmsh
gtm global-settings Module Components

- Introducing the gtm global-settings module
- Alphabetical list of components
Introducing the gtm global-settings module

You can use the `tmsh` components that reside within the `gtm global-settings` module to configure general, load balancing, and metrics settings for the Global Traffic Manager™. You can also configure the metrics address exclusions list. For more information about the `tmsh` hierarchical structure, see Chapter 2, *Understanding and Using the Traffic Management Shell*.

Alphabetical list of components

The remainder of this chapter lists the `tmsh` components that are available in the `gtm global-settings` module.
general

Configures general settings for the Global Traffic Manager.

Module

gtm global-settings

Syntax

Modify or display the general component within the gtm global-settings module using the following syntax.

Modify

modify general
  options:
  auto-discovery [no | yes]
  auto-discovery-interval [integer]
  cache-ldns-servers [no | yes]
  domain-name-check [allow-underscore | idn-compatible | none | strict]
  drain-persistent-requests [no | yes]
  gtm-sets-recursion [no | yes]
  heartbeat-interval [integer]
  monitor-disabled-objects [no | yes]
  send-wildcard-rrs [enable | disable]
  static-persist-cidr-ipv4 [integer]
  static-persist-cidr-ipv6 [integer]
  synchronization [no | yes]
  synchronization-group-name [name]
  synchronization-time-tolerance [integer]
  synchronization-timeout [integer]
  synchronize-zone-files [no | yes]
  synchronize-zone-files-timeout [integer]
  topology-allow-zero-scores [no | yes]
  virtuals-depend-on-server-state [no | yes]
  peer-leader [name]

edit general
  options:
    all-properties
    non-default-properties
    one-line
Display

```
list
list general
show running-config general
show running-config general [option name]
  options:
    all-properties
    non-default-properties
```

Description

You can use the `general` component to modify or display the Global Traffic Manager general settings.

Examples

Turns off auto-discovery for the Global Traffic Manager:
```
modify general auto-discovery no
```

Displays all general properties settings for the Global Traffic Manager:
```
list general all-properties
```

Options

You can use these options with the `general` component:

- **auto-discovery**
  Specifies whether the auto-discovery process is activated for this system. The default value is `no`.

- **auto-discovery-interval**
  Specifies the frequency, in seconds, between system attempts to discover network components. The default value is `30`.

- **cache-ldns-servers**
  Specifies whether the system retains, in the cache, all local DNS servers that make requests. The default value is `yes`.
  **Important:** You must enable this option if you want the system to store and use the LDNS path information.

- **domain-name-check**
  Specifies the parameters for the Global Traffic Manager to use when performing domain name checking. The default value is `strict`.
  The options are:
  - **allow-underscore**
    Underscores are allowed in domain names.
• **idn-compatible**
  International domain names are allowed.

• **none**
  Domain names are not allowed.

• **strict**
  The Global Traffic Manager checks domain names according to the specifications in *RFC 1123 Requirements for Internet Hosts - Application and Support*.

◆ **drain-persistent-requests**
  Specifies, when set to `yes`, that when you disable a pool, load-balanced, persistent connections remain connected until the TTL expires. The default value is `yes`. If you set this option to `no`, any persistent connections terminate immediately when a pool is disabled.

◆ **gtm-sets-recursion**
  Specifies, when set to `yes`, that the system enables recursive DNS queries, regardless of whether the requesting local DNS enabled recursive queries. The default value is `no`.

◆ **heartbeat-interval**
  Specifies the frequency at which the Global Traffic Manager® queries other BIG-IP® systems for updated data. When you are configuring monitors for BIG-IP systems, F5 Networks recommends that you set the `probe-interval` option for the monitor to be equal to or greater than this option. The default value is 10.

◆ **monitor-disabled-objects**
  Specifies, when set to `yes`, that the system continues to monitor objects even if the objects are disabled. The default value is `no`.

◆ **static-persist-cidr-ipv4**
  Specifies the number of bits of the IPv4 address that the system considers when using the Static Persist load balancing mode. The default value is 32.

◆ **static-persist-cidr-ipv46**
  Specifies the number of bits of the IPv6 address that the system considers when using the Static Persist load balancing mode. The default value is 128.

◆ **synchronization**
  Specifies whether this system is a member of a synchronization group. The default value is `no`.

  Members of the synchronization group share configuration and metrics collection information. The synchronization group can contain Global Traffic Manager and Link Controller™ systems.

◆ **synchronization-group-name**
  Specifies the name of the synchronization group to which the system belongs. The default name is `default`.

◆ **synchronization-time-tolerance**
  Specifies the number of seconds that one system clock can be out of sync with another system clock in the synchronization group. If the variance
between the clock times is higher than the value of this option, the system resets the clock that is running behind to match the clock with the most recent time.

Possible values are 0 (zero), and 5 through 600. Values 1 through 4 are automatically set to 5, and 0 (zero) turns time synchronization off. The default value is 10 seconds.

*Note:* If you are using NTP to synchronize the clock with a time server, select a time tolerance other than 0 (zero). When you do this, the system uses the `synchronization-time-tolerance` option as a fail-over mechanism if NTP is disabled for any reason.

- **synchronization-timeout**
  Specifies the number of seconds that the system attempts to synchronize the Global Traffic Manager configuration with a synchronization group member. If the synchronization times out, the system tries again. The default value is 180.

- **synchronize-zone-files**
  Specifies whether the system synchronizes zone files among the synchronization group members. The default value is no.

- **synchronize-zone-files-timeout**
  Specifies the number of seconds that a synchronization group member attempts to synchronize its zone files with a synchronization group member. If the synchronization times out, the system tries again. The default value is 300.

- **topology-allow-zero-scores**
  Specifies if topology load-balancing or qos load-balancing with topology enabled will return pool members with zero topology scores. The default value is yes.

- **virtuals-depend-on-server-state**
  Specifies whether the system marks a virtual server down when the server on which the virtual server is configured can no longer be reached using iQuery. The default value is yes.

- **peer-leader**
  Specifies the name of a gtm server which will be used for executing certain functionality, e.g. creating DNSSEC keys.

See also

edit, gtm settings load-balancing, gtm settings metrics, gtm settings metrics-address-exclusions, list, modify, show, tmsh
load-balancing

Configures load balancing settings for the Global Traffic Manager.

Module

gtm global-settings

Syntax

Modify or display the load-balancing component within the gtm global-settings module using the following syntax.

Modify

edit load-balancing
  options:
    all-properties
    non-default-properties
modify load-balancing
  options:
    ignore-path-ttl [no | yes]
    respect-fallback-dependency [no | yes]
    topology-longest-match [no | yes]
    verify-vs-availability [no | yes]

Display

list
list load-balancing
show running-config load-balancing
show running-config load-balancing [option]
  options:
    all-properties
    non-default-properties
    one-line

Description

You can use the load-balancing component to modify or display the load balancing settings for the Global Traffic Manager.
Examples

Specifies that dynamic load balancing methods can use path data, even after the time-to-live (TTL) for the path data expires:

```
modify load-balancing ignore-path-ttl yes
```

Displays all properties of the load balancing settings for the Global Traffic Manager:

```
list load-balancing all-properties
```

Options

You can use these options with the `load-balancing` component:

- **ignore-path-ttl**
  Specifies, when set to `yes`, that dynamic load balancing methods can use path data, even after the time-to-live (TTL) for the path data expires. The default value is `no`.

- **respect-fallback-dependency**
  Specifies, when set to `yes`, that the system accepts virtual server status when the load balancing mode changes to the mode specified by the `fallback-mode` option of the pool. The default value is `no`.

- **topology-longest-match**
  Specifies, when set to `yes`, that the system evaluates all topology records in the topology statement, and then selects the topology record that most specifically matches the IP address in an LDNS request (in other words, has the longest match). When this option is set to `no`, the system selects the first record in the topology statement that matches the request.

- **verify-vs-availability**
  Specifies, when set to `yes`, that the system checks the availability of virtual servers before sending a connection to those virtual servers. The default value is `no`.

See also

`edit`, `gtm global-settings general`, `gtm global-settings metrics`, `gtm global-settings metrics-address-exclusions`, `list`, `modify`, `show`, `tmsh`
metrics

Configures metrics for the Global Traffic Manager.

Module

gtm global-settings

Syntax

Modify or display the metrics component within the gtm global-settings module using the following syntax.

Modify

modify metrics
  options:
    default-probe-limit [integer]
    hops-ttl [integer]
    hops-packet-length [integer]
    hops-sample-count [integer]
    hops-timeout [integer]
    inactive-ldns-ttl [integer]
    inactive-paths-ttl [integer]
    max-synchronous-monitor-requests [integer]
    metrics-caching [integer]
    metrics-collection-protocols none
    metrics-collection-protocols
      [add | delete | replace-all-with] {
        [dns-dot | dns-rev | icmp | tcp | udp] ...
      }
    path-ttl [integer]
    paths-retry [integer]

edit metrics
  options:
    all-properties
    non-default-properties

Display

list

list metrics

show running-config metrics

show running-config metrics [option]
options:
  all-properties
  non-default-properties
  one-line

Description

You can use the metrics component to modify or display the Global Traffic Manager metrics settings.

Examples

Sets the default probe limit for the Global Traffic Manager to 10:
modify metrics default-probe-limit 10

Displays all properties of the metrics settings for the Global Traffic Manager:
list metrics all-properties

Options

You can use these options with the metrics component:

- **default-probe-limit**
  Specifies the number of probe attempts that the system performs before removing the path from the metrics. The default value is 12.

- **hops-ttl**
  Specifies the number of seconds that the system considers traceroute utility data to be valid for name resolution and load balancing. The default value is 604800. This option must be greater than the hops-timeout option.

- **hops-packet-length**
  Specifies the length of packets, in bytes, that the system sends to a local DNS server to determine the path information between the two systems. The default value is 64.

- **hops-sample-count**
  Specifies the number of packets that the system sends to a local DNS server to determine the path information between those two systems. The default value is 3.

- **hops-timeout**
  Specifies the number of seconds that the big3d daemon waits for a probe. The default value is 3.
inactive-ldns-ttl
Specifies the number of seconds that an inactive LDNS remains in the cache. Each time an LDNS makes a request, the clock starts again. Valid values are 60 through 4294967295. The default value is 2419200 (28 days).

inactive-paths-ttl
Specifies the number of seconds that a path remains in the cache after its last access. Valid values are 60 through 4294967295. The default value is 604800 (7 days).

max-synchronous-monitor-requests
Specifies how many monitors can attempt to verify the availability of a given resource at the same time. The default value is 20.

metrics-caching
Specifies the interval (in seconds) at which the system dumps path and other metrics data. Valid values are 0 through 604800. The default value is 3600; 0 (zero) turns this feature off.

metrics-collection-protocols
Specifies the protocols that the system uses to collect metrics information relevant to LDNS servers.

path-ttl
Specifies the number of seconds that the system considers path data to be valid for name resolution and load balancing purposes. The default value is 2400. This option must be greater than the paths-retry option.

paths-retry
Specifies the interval (in seconds) at which the system retries the path data. The default value is 120.

See also
edit, gtm global-settings general, gtm global-settings load-balancing, gtm global-settings metrics-address-exclusions, list, modify, show, tmsh
metrics-exclusions

  Configures the IP addresses that you want to exclude from the Global Traffic Manager metrics.

Module

  gtm global-settings

Syntax

  Modify or display the metrics-exclusions component within the gtm global-settings module using the following syntax.

Modify

  modify metrics-exclusions
  
  options:
  
  addresses [add | delete | none | replace-all-with] { [ip address]... }

  edit metrics-exclusion
  
  options:
  
  all-properties

Display

  list
  
  list metrics-exclusions
  
  show running-config metrics-exclusions
  
  address
  
  options:
  
  all-properties
  
  one-line

Description

  You can use the metrics-exclusions component to exclude IP addresses from the Global Traffic Manager metrics.
Examples

Excludes the IP address **10.10.10.1** from the Global Traffic Manager metrics:

```
modify metrics-exclusions addresses add {10.10.10.1}
```

Displays the IP addresses that are excluded from the Global Traffic Manager metrics:

```
list metrics-exclusions
```

Options

You can use this option with the `settings` component:

- **ip address**
  Specifies the IP addresses that you want to add to or delete from the exclusion list, or with which you want to replace all existing IP addresses that are currently on the exclusion list.

See also

```
edit, gtm global-settings general, gtm global-settings load-balancing, gtm global-settings metrics, list, modify, show, tmsh
```
gtm monitor Module Components

• Introducing the gtm monitor module
• Alphabetical list of components
Introducing the gtm monitor module

You can use the tmsh components that reside within the gtm monitor module to configure Global Traffic Manager™ monitors. For more information about the tmsh hierarchical structure, see Chapter 2, *Understanding and Using the Traffic Management Shell*. For more information about configuring monitors, refer to the *Configuration Guide for BIG-IP® Global Traffic Manager™*.

Alphabetical list of components

The remainder of this chapter lists the tmsh components that are available in the gtm monitor module.
bigip

Configures a BIG-IP® monitor.

Module

gtm monitor

Syntax

Configure the bigip component within the gtm monitor module using the following syntax.

Create/Modify

create bigip [name]
modify bigip [name]

options:
-aggregate-dynamic-ratios [average-members | average-nodes | none | sum-members | \ sum-nodes]
-defaults-from [name]
-description [string]
-destination [ip address][port]
-ignore-down-response [enabled | disabled]
-interval [integer]
-timeout [integer]

edit bigip [ [name] | [glob] | [regex] ] ...

options:
-all-properties
-non-default-properties

Display

list bigip
list bigip [ [name] | [glob] | [regex] ] ...

show running-config bigip

show running-config bigip [ [name] | [glob] | [regex] ] ...

options:
-all-properties
-non-default-properties
-one-line
-partition
Delete

delete bigip [name]

◆ Note
You cannot delete default monitors.

Description

You can use the bigip component in the gtm monitor module to configure a custom monitor, or you can use the default pre-configured BIG-IP monitor that the Global Traffic Manager provides. This type of monitor acquires data captured through monitors managed by a Local Traffic Manager™. The BIG-IP monitor is both a health and performance monitor. You can monitor only the following components with a BIG-IP monitor:
- Global Traffic Manager server
- Global Traffic Manager virtual server
- Local Traffic Manager server
- Local Traffic Manager virtual server

Examples

Creates a monitor named my_bigip that inherits properties from the default BIG-IP monitor:
create bigip my_bigip defaults-from bigip

Displays the properties of all of the BIG-IP monitors:
list bigip

Options

You can use these options with the bigip component:

◆ aggregate-dynamic-ratios
Specifies the monitor’s response to a query. By default, the BIG-IP monitor uses the gtm_score value as the vs_score for a Local Traffic Manager virtual server.

You can use this option to override the default behavior using the following values:

- average-members
Specifies that the monitor uses as a response to a query the average of the dynamic ratio values of the pool members associated with the pools that are associated with the virtual server.
• **average-nodes**
  Specifies that the monitor uses as a response to a query the average value of all of the nodes associated with the pool members that are associated with the pools that are associated with the virtual server.

• **none**
  This is the default value.

• **sum-members**
  Specifies that the monitor uses the sum of the pool members as a response to a query.

• **sum-nodes**
  Specifies that the monitor uses the sum of the dynamic ratios of all of the nodes as a response to a query.

◆ **defaults-from**
  Specifies the name of the monitor from which you want your custom monitor to inherit settings. The default value is `bigip`.

◆ **description**
  User-defined description.

◆ **destination**
  Specifies the IP address and service port of the resource that is the destination of this monitor. The default value is `*: *`.
  Possible values are:
  • `*: *`
    Specifies that the system marks a virtual server **up** or **down** based on the response of the virtual server at the IP address and port supplied by the virtual server.
  • `*: port`
    Specifies that the system marks a virtual server **up** or **down** based on the response of the virtual server at the IP address supplied by the virtual server and the port you specify.
  • `<IP address>:<port>`
    Specifies that the system marks a virtual server **up** or **down** based on the response of the virtual server at the IP address and port you specify.

◆ **glob**
  Displays the items that match the glob expression. For a description of glob expression syntax, see the glob man page.

◆ **ignore-down-response**
  Specifies whether the monitor ignores a down response from the system it is monitoring. The default value is **disabled**.

◆ **interval**
  Specifies the frequency at which the system issues the monitor check. The default value is 30 seconds.

◆ **name**
  Specifies a unique name for the component. This option is required for the commands **create**, **delete**, and **modify**.
◆ **partition**
   Displays the administrative partition in which the component resides.

◆ **regex**
   Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. For a description of regular expression syntax, see the **regex** man page.

◆ **timeout**
   Specifies the number of seconds the target has in which to respond to the monitor request. The default value is **90** seconds.
   
   If the target responds within the set time period, it is considered up. If the target does not respond within the set time period, it is considered down. Also, if the target responds with a RESET packet, the system immediately flags the target as down without waiting for the timeout interval to expire.

**See also**

create, delete, edit, glob, gtm pool, gtm server, list, modify, regex show, tmsh


**bigip-link**

Configures a BIG-IP Link monitor.

**Module**

`gtm monitor`

**Syntax**

Configure the `bigip-link` component within the `gtm monitor` module using the following syntax.

**Create/Modify**

```plaintext
create bigip-link [name]
modify bigip-link [name]
  options:
    defaults-from [name]
    description [string]
    destination [ip address]
    ignore-down-response [enabled | disabled]
    interval [integer]
    timeout [integer]
edit bigip-link [ [name] | [glob] | [regex] ] ...
  options:
    all-properties
    non-default properties
```

**Display**

```plaintext
list bigip-link
list bigip-link [ [name] | [glob] | [regex] ] ...
show running-config bigip-link
show running-config bigip-link [ [name] | [glob] | [regex] ] ...
  options:
    all-properties
    non-default-properties
    one-line
    partition
```
Delete

```
delete bigip-link [name]
```

◆ **Note**

*You cannot delete default monitors.*

Description

You can use the `bigip-link` component to configure a custom monitor, or you can use the default BIG-IP Link monitor that the Global Traffic Manager provides. This type of monitor acquires data captured through monitors managed by a BIG-IP Link Controller™.

Examples

Creates a monitor named `my_bigip-link` that inherits properties from the default BIG-IP Link monitor:

```
create bigip-link my_bigip-link defaults-from bigip_link
```

Displays the properties of all of the BIG-IP Link monitors:

```
list bigip-link
```

Options

You can use these options with the `bigip-link` component:

◆ **defaults-from**
  Specifies the name of the monitor from which you want your custom monitor to inherit settings. The default value is `bigip_link`.

◆ **description**
  User-defined description.

◆ **destination**
  Specifies the IP address of the resource that is the destination of this monitor. The default value is `*`.

Possible values are:

- `*`
  Specifies that the system performs a health check on the IP address of the node.

- `<IP address>`
  Specifies that the system performs a health check on the IP address that you specify, routes the check through the IP address of the associated node, and marks the IP address of the associated node `up` or `down` accordingly.
◆ **glob**  
Displays the items that match the `glob` expression. For a description of `glob` expression syntax, see the `glob` man page.

◆ **ignore-down-response**  
Specifies whether the monitor ignores a down response from the system it is monitoring. The default value is `disabled`.

◆ **interval**  
Specifies the frequency at which the system issues the monitor check. The default value is 10 seconds.

◆ **name**  
Specifies a unique name for the component. This option is required for the commands `create`, `delete`, and `modify`.

◆ **partition**  
Displays the administrative partition in which the component resides.

◆ **regex**  
Displays the items that match the regular expression. The regular expression must be preceded by an at sign (`@[regular expression]`) to indicate that the identifier is a regular expression. See `help regex` for a description of regular expression syntax.

◆ **timeout**  
Specifies the number of seconds the target has in which to respond to the monitor request. The default value is 30 seconds.

If the target responds within the set time period, it is considered **up**. If the target does not respond within the set time period, it is considered **down**. Also, if the target responds with a RESET packet, the system immediately flags the target as **down** without waiting for the timeout interval to expire.

**See also**

`create`, `delete`, `edit`, `glob`, `gtm link`, `list`, `ltm node`, `modify`, `regex`, `show`, `tmsh`
external

Configures an external monitor.

Module

gtm monitor

Syntax

Configure the `external` component within the `gtm monitor` module using the following syntax.

Create/Modify

```bash
create external [name]
modify external [name]
options:
  args [ [arguments] | none]
  defaults-from [name]
  description [string]
  destination [ip address][port]
  ignore-down-response [enabled | disabled]
  interval [integer]
  probe-timeout [integer]
  run [none | [path] ]
  timeout [integer]
  user-defined [ [name] [value] | [name] none ]
```

```bash
edit external [ [name] | [glob] | [regex] ] ...
options:
  all-properties
  non-default properties
```

Display

```bash
list external
list external [ [name] | [glob] | [regex] ] ...
show running-config external
show running-config external [ [name] | [glob] | [regex] ] ...
options:
  all-properties
  non-default-properties
  one-line
  partition
```
Delete

```
delte external [name]
```

◆ Note

*You cannot delete default monitors.*

Description

You can use the `external` component to configure a custom monitor, or you can use the default external monitor that the Global Traffic Manager provides. You can use this type of monitor to monitor services using your own programs.

Examples

Creates a monitor named `my_external` that inherits properties from the default external monitor:

```
create external my_external defaults-from external
```

Displays the properties of all of the external monitors:

```
list external
```

Options

You can use these options with the `external` component:

- **args**
  Specifying any command line arguments that the external program requires. The default value is `none`.

- **defaults-from**
  Specifies the name of the monitor from which you want your custom monitor to inherit settings. The default value is `external`.

- **description**
  User-defined description.

- **destination**
  Specifies the IP address and service port of the resource that is the destination of this monitor. The default value is `*:*`.

  Possible values are:

  - `*:*`
    Specifies that the system marks a pool member **up** or **down** based on the response of the server at the IP address and port supplied by the pool member.
• \*:port
  Specifies that the system marks a pool member up or down based on the response of the server at the IP address supplied by the pool member and the port you specify.

• <IP address>:<port>
  Specifies that the system marks a pool member up or down based on the response of the server at the IP address and port you specify.

◆ glob
  Displays the items that match the glob expression. For a description of glob expression syntax, see the glob man page.

◆ ignore-down-response
  Specifies whether the monitor ignores a down response from the system it is monitoring. The default value is disabled.

◆ interval
  Specifies the frequency at which the system issues the monitor check. The default value is 30 seconds.

◆ name
  Specifies a unique name for the component. This option is required for the commands create, delete, and modify.

◆ partition
  Displays the administrative partition in which the component resides.

◆ probe-timeout
  Specifies the number of seconds after which the BIG-IP system times out the probe request to the BIG-IP system. The default value is 5 seconds.

◆ regex
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. For a description of regular expression syntax, see the regex man page.

◆ run
  Specifies the path and file name of a program to run as the external monitor, for example /config/monitors/myMonitor. The default value is none.

◆ timeout
  Specifies the number of seconds the target has in which to respond to the monitor request. The default value is 120 seconds.

  If the target responds within the set time period, it is considered up. If the target does not respond within the set time period, it is considered down. Also, if the target responds with a RESET packet, the system immediately flags the target as down without waiting for the timeout interval to expire.

◆ user-defined
  Specifies any user-defined command-line arguments and variables that the external program requires.

  Use the following syntax to specify a user-defined parameter:

  ```
  modify external my_external user-defined my_param_name my_param_value
  ```
Use the following syntax to remove a user-defined parameter:

```shell
modify external my_external user-defined my_param_name none.
```

**See also**

create, delete, edit, glob, gtm pool, list, modify, regex show, tmsh
firepass

Configures a FirePass® monitor.

Module

gtm monitor

Syntax

Configure the firepass component within the gtm monitor module using the following syntax.

Create/Modify

create firepass [name]
modify firepass [name]
    options:
        check-until-up [enabled | disabled]
        cipherlist [list]
        concurrency-limit [integer]
        defaults-from [name]
        description [string]
        destination [ip address][port]
        ignore-down-response [enabled | disabled]
        interval [integer]
        manual-resume [enabled | disabled]
        max-load-average [integer]
        password [none | [password]]
        probe-timeout [integer]
        timeout [integer]
        username [ [name] | none]
    edit firepass [ [ [name] | [glob] | [regex] ] ... ]
    options:
        all-properties
        non-default-properties

Display

list firepass
list firepass [ [ [name] | [glob] | [regex] ] ... ]
show running-config firepass
show running-config firepass [ [ [name] | [glob] | [regex] ] ... ]
Chapter 21

options:
  all-properties
  non-default-properties
  one-line
  partition

Delete

delete firepass [name]

◆ Note

You cannot delete default monitors.

Description

You can use the firepass component to configure a custom monitor, or you can use the default FirePass monitor that the BIG-IP Global Traffic Manager provides. The FirePass monitor is both a health and performance monitor.

Examples

Creates a monitor named my_firepass that inherits properties from the default FirePass monitor.

create firepass my_firepass defaults-from firepass

Displays the properties of all of the FirePass monitors:

list firepass

Options

You can use these options with the firepass component:

◆ cipherlist
  Specifies a cipher list. If you do not specify a cipher list, the monitor uses the default cipher list HIGH:!ADH.

◆ concurrency-limit
  Specifies the maximum percentage of licensed connections currently in use under which the monitor marks the FirePass system up. As an example, a value of 95 percent means that the monitor marks the FirePass system up until 95 percent of licensed connections are in use. When the number of in-use licensed connections exceeds 95 percent, the monitor marks the FirePass system down. The default value is 95.

◆ defaults-from
  Specifies the name of the monitor from which you want your custom monitor to inherit settings. The default value is firepass.
gtm monitor Module Components

- **description**
  User-defined description.

- **destination**
  Specifies the IP address and service port of the resource that is the destination of this monitor. The default value is ":*".
  Possible values are:
  - ":*"
    Specifies that the system marks a pool member **up** or **down** based on the response of the server at the IP address and port supplied by the pool member.
  - ":port"
    Specifies that the system marks a pool member **up** or **down** based on the response of the server at the IP address supplied by the pool member and the port you specify.
  - `<IP address>:<port>`
    Specifies that the system marks a pool member **up** or **down** based on the response of the server at the IP address and port you specify.

- **glob**
  Displays the items that match the **glob** expression. For a description of **glob** expression syntax, see the **glob** man page.

- **ignore-down-response**
  Specifies whether the monitor ignores a down response from the system it is monitoring. The default value is **disabled**.

- **interval**
  Specifies the frequency at which the system issues the monitor check. The default value is **5** seconds.

- **max-load-average**
  Specifies the number that the monitor uses to mark the FirePass system **up** or **down**. The system compares the value of this option to a one-minute average of the FirePass system load. When the FirePass system-load average falls within the specified Max Load Average value, the monitor marks the FirePass system **up**. When the average exceeds the value, the monitor marks the system **down**. The default value is **12**.

- **name**
  Specifies a unique name for the component. This option is required for the commands **create**, **delete**, and **modify**.

- **partition**
  Displays the administrative partition in which the component resides.

- **password**
  Specifies the password, if the monitored target requires authentication. The default value is **none**.

- **probe-timeout**
  Specifies the number of seconds after which the BIG-IP system times out the probe request to the BIG-IP system. The default value is **5** seconds.
◆ regex
Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. For a description of regular expression syntax, see the regex man page.

◆ timeout
Specifies the number of seconds the target has in which to respond to the monitor request. The default value is 90 seconds.

If the target responds within the set time period, it is considered up. If the target does not respond within the set time period, it is considered down. Also, if the target responds with a RESET packet, the system immediately flags the target as down without waiting for the timeout interval to expire.

◆ username
Specifies the user name if the monitored target requires authentication. The default value is gtmuser.

See also
create, delete, edit, glob, list, modify, regex, show, tmsh
**ftp**

Configures a File Transfer Protocol (FTP) monitor.

**Module**

`gtm monitor`

**Syntax**

Configure the `ftp` component within the `gtm monitor` module using the following syntax.

**Create/Modify**

```bash
create ftp [name]
modify ftp [name]
```

options:
- `debug [no | yes]`
- `defaults-from [name]`
- `description [string]`
- `destination [ip address][port]`
- `filename [ [filename] | none]`
- `ignore-down-response [enabled | disabled]`
- `interval [integer]`
- `mode [passive | port]`
- `password [none | [password] ]`
- `probe-timeout [integer]`
- `timeout [integer]`
- `username [name]`

```bash
edit ftp [ [name] | [glob] | [regex] ] ... ]
```

options:
- `all-properties`
- `non-default-properties`

**Display**

```bash
list ftp
list ftp [ [name] | [glob] | [regex] ] ... ]
show running-config ftp
show running-config ftp [ [name] | [glob] | [regex] ] ... ]
```

options:
- `all-properties`
- `non-default-properties`
- `one-line`
- `partition`
Delete

```bash
delete ftp [name]
```

◆ Note

You cannot delete default monitors.

Description

You can use the `ftp` component to configure a custom monitor, or you can use the default FTP monitor that the Global Traffic Manager provides. This type of monitor verifies the FTP service by attempting to download a specific file to the `/var/tmp` directory on the system. Once downloaded successfully, the file is not saved.

Examples

Creates a monitor named `my_ftp` that inherits properties from the default FTP monitor:

```bash
create ftp my_ftp defaults-from ftp
```

Displays the properties of all of the FTP monitors:

```bash
list ftp
```

Options

You can use these options with the `ftp` component:

◆ `debug`
  Specifies whether the monitor sends error messages and additional information to a log file created and labeled specifically for this monitor. You can use the log information to help diagnose and troubleshoot unsuccessful health checks. The default value is `no`.

  The options are:
  
  * `no`
    Specifies that the system does not redirect error messages and additional information related to this monitor.
  
  * `yes`
    Specifies that the system redirects error messages and additional information to the `/var/log/<monitor_type>_<ip address>_<port>.log` file.

◆ `defaults-from`
  Specifies the name of the monitor from which you want your custom monitor to inherit settings. The default value is `ftp`.

◆ `description`
  User-defined description.
◆ **destination**
   Specifies the IP address and service port of the resource that is the destination of this monitor. The default value is `*::*`.
   Possible values are:
   - `*::*`
     Specifies that the system marks a pool member **up** or **down** based on the response of the server at the IP address and port supplied by the pool member.
   - `*:port`
     Specifies that the system marks a pool member **up** or **down** based on the response of the server at the IP address supplied by the pool member and the port you specify.
   - `<IP address>:<port>`
     Specifies that the system marks a pool member **up** or **down** based on the response of the server at the IP address and port you specify.

◆ **filename**
   Specifies the full path and file name of the file that the system attempts to download. The health check is successful if the system can download the file. The default value is **none**.

◆ **glob**
   Displays the items that match the **glob** expression. For a description of **glob** expression syntax, see the **glob** man page.

◆ **ignore-down-response**
   Specifies whether the monitor ignores a down response from the system it is monitoring. The default value is **disabled**.

◆ **interval**
   Specifies the frequency at which the system issues the monitor check. The default value is **10** seconds.

◆ **mode**
   Specifies the data transfer process (DTP) mode. The default value is **passive**.
   The options are:
   - **passive**
     Specifies that the monitor sends a data transfer request to the FTP server. When the FTP server receives the request, the FTP server then starts and establishes the data connection.
   - **port**
     Specifies that the monitor starts and establishes the data connection with the FTP server.

◆ **name**
   Specifies a unique name for the component. This option is required for the commands **create**, **delete**, and **modify**.

◆ **password**
   Specifies the password, if the monitored target requires authentication. The default value is **none**.
partition
Displays the administrative partition in which the component resides.

probe-timeout
Specifies the number of seconds after which the BIG-IP system times out
the probe request to itself. The default value is 5 seconds.

regex
Displays the items that match the regular expression. The regular
expression must be preceded by an at sign (@[regular expression]) to
indicate that the identifier is a regular expression. For a description of
regular expression syntax, see the regex man page.

timeout
Specifies the number of seconds the target has in which to respond to the
monitor request. The default value is 31 seconds.

If the target responds within the set time period, it is considered up. If the
target does not respond within the set time period, it is considered down.
Also, if the target responds with a RESET packet, the system
immediately flags the target as down without waiting for the timeout
interval to expire.

username
Specifies the user name if the monitored target requires authentication.
The default value is none.

See also

create, delete, edit, glob, gtm pool, list, modify, regex show, tmsh
### gateway-icmp

Configures a Gateway Internet Control Message Protocol (ICMP) monitor.

**Module**

```
gtm monitor
```

**Syntax**

Configure the `gateway-icmp` component within the `gtm monitor` module using the following syntax.

**Create/Modify**

```
create gateway-icmp [name]
mist gateway-icmp [name]
options:
  defaults-from [name]
  description [string]
  destination [ip address][port]
  ignore-down-response [enabled | disabled]
  interval [integer]
  probe-attempts [integer]
  probe-interval [integer]
  probe-timeout [integer]
  timeout [integer]
  transparent [enabled | disabled]
```

```
edit gateway-icmp [ [name] | [glob] | [regex] ] ... ]
options:
  all-properties
  non-default properties
```

**Display**

```
list gateway-icmp
list gateway-icmp [ [name] | [glob] | [regex] ] ... ]
show running-config gateway-icmp
show running-config gateway-icmp [ [name] | [glob] | [regex] ] ... ]
options:
  all-properties
  non-default-properties
  one-line
  partition
```
Delete

```
delete gateway-icmp [name]
```

◆ Note

You cannot delete default monitors.

Description

You can use the `gateway-icmp` component to configure a custom monitor, or you can use the default Gateway ICMP monitor that the Global Traffic Manager provides. This type of monitor inspects a pool that implements gateway fail-safe for high availability.

Examples

Creates a monitor named `my_icmp` that inherits properties from the default Gateway ICMP monitor:

```
create gateway-icmp my_icmp defaults-from gateway_icmp
```

Displays the properties of all of the Gateway ICMP monitors:

```
list gateway-icmp
```

Options

You can use these options with the `gateway-icmp` component:

◆ **defaults-from**
Specifies the name of the monitor from which you want your custom monitor to inherit settings. The default value is `gateway_icmp`.

◆ **description**
User-defined description.

◆ **destination**
Specifies the IP address and service port of the resource that is the destination of this monitor. The default value is `*:`.

Possible values are:

- `*:`
  Specifies that the system marks a pool member up or down based on the response of the server at the IP address and port supplied by the pool member.

- `*:port`
  Specifies that the system marks a pool member **up** or **down** based on the response of the server at the IP address supplied by the pool member and the port you specify.
• `<IP address>:<port>`
  Specifies that the system marks a pool member **up** or **down** based on the response of the server at the IP address and port you specify.

• `<IP address>:<port>` (with the **transparent** option **enabled**)
  Specifies that the system performs a health check on the server at the IP address and port you specify, routes the check through the IP address and port supplied by the pool member, and marks the pool member (the gateway) **up** or **down** accordingly.

  ◆ **glob**
  Displays the items that match the **glob** expression. For a description of **glob** expression syntax, see the **glob** man page.

  ◆ **ignore-down-response**
  Specifies whether the monitor ignores a down response from the system it is monitoring. The default value is **disabled**.

  ◆ **interval**
  Specifies the frequency at which the system issues the monitor check. The default value is **30** seconds.

  ◆ **name**
  Specifies a unique name for the component. This option is required for the commands **create**, **delete**, and **modify**.

  ◆ **partition**
  Displays the administrative partition in which the component resides.

  ◆ **probe-attempts**
  Specifies the number of times the BIG-IP system attempts to probe the host server, after which the BIG-IP system considers the host server **down** or unavailable. The default value is **3** attempts.

  ◆ **probe-interval**
  Specifies the frequency at which the BIG-IP system probes the host server. The default value is **1** second.

  ◆ **probe-timeout**
  Specifies the number of seconds after which the BIG-IP system times out the probe request to the BIG-IP system. The default value is **5** seconds.

  ◆ **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. For a description of regular expression syntax, see the **regex** man page.

  ◆ **timeout**
  Specifies the number of seconds the target has in which to respond to the monitor request. The default value is **120** seconds.

    If the target responds within the set time period, it is considered **up**. If the target does not respond within the set time period, it is considered **down**. Also, if the target responds with a RESET packet, the system immediately flags the target as **down** without waiting for the timeout interval to expire.
◆ transparent
Specifies whether the monitor operates in transparent mode. Monitors in transparent mode can monitor pool members through firewalls. The default value is disabled.

See also

create, delete, edit, glob, gtm link, gtm pool, gtm server, list, modify, regex, show, tmsh
http

Configures a Hypertext Transfer Protocol (HTTP) monitor.

Module

gtm monitor

Syntax

Configure the http component within the gtm monitor module using the following syntax.

Create/Modify

create http [name]
modify http [name]
options:
  defaults-from [name]
  description [string]
  destination [ip address][port]
  ignore-down-response [enabled | disabled]
  interval [integer]
  password [none | [password] ]
  probe-timeout [integer]
  recv [none | [string] ]
  reverse [enabled | disabled]
  send [none | [string] ]
  timeout [integer]
  transparent [enabled | disabled]
  username [ [name] | none]
edit http [ [name] | [glob] | [regex] ] ... ]
options:
  all-properties
  non-default properties

Display

list http
list http [ [name] | [glob] | [regex] ] ... ]
show running-config http
show running-config http [ [name] | [glob] | [regex] ] ... ]
options:
  all-properties
non-default-properties
one-line
partition

Delete

delete http [name]

◆ Note

You cannot delete default monitors.

Description

You can use the http component to configure a custom monitor, or you can use the default HTTP monitor that the Global Traffic Manager provides. This type of monitor verifies the HTTP service by attempting to receive specific content from a web page.

Examples

Creates a monitor named my_http that inherits properties from the default HTTP monitor:

create http my_http defaults-from http

Displays the properties of all of the HTTP monitors:

list http

Options

You can use these options with the http component:

◆ defaults-from
   Specifies the name of the monitor from which you want your custom monitor to inherit settings. The default value is http.

◆ description
   User-defined description.

◆ destination
   Specifies the IP address and service port of the resource that is the destination of this monitor. The default value is *:*.

   Possible values are:
   • *:*  
     Specifies that the system marks a pool member up or down based on the response of the server at the IP address and port supplied by the pool member.
gtm monitor Module Components

- *:port
  Specifies that the system marks a pool member up or down based on the response of the server at the IP address supplied by the pool member and the port you specify.

- <IP address>:<port>
  Specifies that the system marks a pool member up or down based on the response of the server at the IP address and port you specify.

- <IP address>:<port> (with the transparent option enabled)
  Specifies that the system performs a health check on the server at the IP address and port you specify, routes the check through the IP address and port supplied by the pool member, and marks the pool member (the gateway) up or down accordingly.

- glob
  Displays the items that match the glob expression. For a description of glob expression syntax, see the glob man page.

- ignore-down-response
  Specifies whether the monitor ignores a down response from the system it is monitoring. The default value is disabled.

- interval
  Specifies the frequency at which the system issues the monitor check. The default value is 30 seconds.

- name
  Specifies a unique name for the component. This option is required for the commands create, delete, and modify.

- partition
  Displays the administrative partition in which the component resides.

- password
  Specifies the password if the monitored target requires authentication. The default value is none.

- probe-timeout
  Specifies the number of seconds after which the BIG-IP system times out the probe request to itself. The default value is 5 seconds.

- recv
  Specifies the text string that the monitor looks for in the returned resource. The default value is none. The most common receive expressions contain a text string that is included in an HTML file on your site. The text string can be regular text, HTML tags, or image names. If you do not specify a value for both the send and recv options, the monitor performs a simple service check and connect only.

- regex
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. For a description of regular expression syntax, see the regex man page.
◆ **reverse**
Specifies whether the monitor operates in reverse mode. When the monitor is in reverse mode, a successful check marks the monitored object **down** instead of **up**. You can use the this mode only if you configure both the **send** and **recv** options.

The default value is **disabled**, which specifies that the monitor does not operate in reverse mode. The **enabled** value specifies that the monitor operates in reverse mode.

◆ **send**
Specifies the text string that the monitor sends to the target object.

The default value is **GET /**, which retrieves a default HTML file for a web site. To retrieve a specific page from a web site, specify a fully-qualified path name, for example:

```
GET /www/company/index.html.
```

Since the string can have special characters, the system can require that the string be enclosed with single quotation marks.

If this value is null, then a valid connection suffices to determine that the service is **up**. In this case, the system does not need the **recv** option and ignores the option even if not null.

◆ **timeout**
Specifies the number of seconds the target has in which to respond to the monitor request. The default value is **120** seconds.

If the target responds within the set time period, it is considered **up**. If the target does not respond within the set time period, it is considered **down**. Also, if the target responds with a RESET packet, the system immediately flags the target as **down** without waiting for the timeout interval to expire.

◆ **transparent**
Specifies whether the monitor operates in transparent mode. Monitors in transparent mode can monitor pool members through firewalls. The default value is **disabled**.

◆ **username**
Specifies the user name if the monitored target requires authentication. The default value is **none**.

**See also**

create, delete, edit, glob, gtm pool, gtm server, list, modify, regex, show, tmsh
**Module**

`gtm monitor`  

**Syntax**

Configure the `https` component within the `gtm monitor` module using the following syntax.

**Create/Modify**

```plaintext
create https [name]
modify https [name]
```

Options:

- `.cert` [cert list] | none
- `.cipherlist` [string]
- `.compatibility` [enabled | disabled]
- `.defaults-from` [name]
- `.description` [string]
- `.destination` [ip address][port]
- `.ignore-down-response` [enabled | disabled]
- `.interval` [integer]
- `.key` [key] | none
- `.password` [none | [password]]
- `.probe-timeout` [integer]
- `.recv` [none | [string]]
- `.reverse` [enabled | disabled]
- `.send` [none | [string]]
- `.timeout` [integer]
- `.transparent` [enabled | disabled]
- `.username` [name] | none

**Display**

```plaintext
list https
```

```plaintext
list https [name] | [glob] | [regex] ...]
```
show running-config https
show running-config https [ [name] | [glob] | [regex] ] ... ]
options:
   all-properties
   non-default-properties
   one-line
   partition

Delete

delete https [name]

◆ Note

You cannot delete default monitors.

Description

You can use the https component to configure a custom monitor, or you can use the default HTTPS monitor that the Global Traffic Manager provides. This type of monitor verifies the HTTPS service by attempting to receive specific content from a web page protected by Secure Socket Layer (SSL) security.

Examples

Creates a monitor named my_https that inherits properties from the default HTTPS monitor:
create https my_https defaults-from https

Displays the properties of all of the HTTPS monitors:
list https

Options

You can use these options with the https component:

◆ cert
   Specifies a fully-qualified path for a client certificate that the monitor sends to the target SSL server. The default value is none.

◆ cipherlist
   Specifies the list of ciphers for this monitor. The default list DEFAULT:+SHA:+3DES:+kEDH is located in the file base_monitors.conf.

◆ compatibility
   Specifies, when enabled, that the SSL options setting (in OpenSSL) is set to ALL. The default value is enabled.
- **defaults-from**
  Specifies the name of the monitor from which you want your custom monitor to inherit settings. The default value is **https**.

- **description**
  User-defined description.

- **destination**
  Specifies the IP address and service port of the resource that is the destination of this monitor. The default value is ***:***.
  Possible values are:
  - ***:***
    Specifies that the system marks a pool member **up** or **down** based on the response of the server at the IP address and port supplied by the pool member.
  - ***:port**
    Specifies that the system marks a pool member **up** or **down** based on the response of the server at the IP address supplied by the pool member and the port you specify.
  - **<IP address>:<port>**
    Specifies that the system marks a pool member **up** or **down** based on the response of the server at the IP address supplied by the pool member and the port you specify.
  - **<IP address>:<port>** (with the **transparent** option enabled)
    Specifies that the system performs a health check on the server at the IP address and port you specify, routes the check through the IP address and port supplied by the pool member, and marks the pool member (the gateway) **up** or **down** accordingly.

- **glob**
  Displays the items that match the **glob** expression. For a description of **glob** expression syntax, see the **glob** man page.

- **ignore-down-response**
  Specifies whether the monitor ignores a down response from the system it is monitoring. The default value is **disabled**.

- **interval**
  Specifies the frequency at which the system issues the monitor check. The default value is **30** seconds.

- **key**
  Specifies the RSA private key if the monitored target requires authentication. The key must be surrounded by quotation marks, for example: **key "client.key"**. If you specify a key, you must also specify a value for the **cert** option. The default value is **none**.

- **name**
  Specifies a unique name for the component. This option is required for the commands **create**, **delete**, and **modify**.

- **partition**
  Displays the administrative partition in which the component resides.
◆ **password**
   Specifies the password if the monitored target requires authentication.
   The default value is none.

◆ **probe-timeout**
   Specifies the number of seconds after which the BIG-IP system times out
   the probe request to the BIG-IP system. The default value is 5 seconds.

◆ **recv**
   Specifies the text string that the monitor looks for in the returned
   resource. The default value is none.

   The most common receive expressions contain a text string that is
   included in an HTML file on your site. The text string can be regular
   text, HTML tags, or image names. If you do not specify a value for both
   the send and recv options, the monitor performs a simple service check
   and connect only.

◆ **regex**
   Displays the items that match the regular expression. The regular
   expression must be preceded by an at sign (@[regular expression]) to
   indicate that the identifier is a regular expression. For a description of
   regular expression syntax, see the regex man page.

◆ **reverse**
   Specifies whether the monitor operates in reverse mode. When the
   monitor is in reverse mode, a successful check marks the monitored
   object down instead of up. You can use the this mode only if you
   configure both the send and recv options.

   The default value is disabled. The disabled value specifies that the
   monitor does not operate in reverse mode. The enabled value specifies
   that the monitor operates in reverse mode.

◆ **send**
   Specifies the text string that the monitor sends to the target object. The
   default value is GET /, which retrieves a default HTML file for a web
   site.

   To retrieve a specific page from a web site, specify a fully-qualified path
   name, for example: GET /www/company/index.html. Since the string
   can have special characters, the system can require that the string be
   enclosed with single quotation marks.

   If this value is null, then a valid connection suffices to determine that the
   service is up. In this case, the system does not need the recv option and
   ignores the option even if not null.

◆ **timeout**
   Specifies the number of seconds the target has in which to respond to the
   monitor request. The default value is 120 seconds.

   If the target responds within the set time period, it is considered up. If the
   target does not respond within the set time period, it is considered down.
   Also, if the target responds with a RESET packet, the system
   immediately flags the target as down without waiting for the timeout
   interval to expire.
◆ **transparent**
  Specifies whether the monitor operates in transparent mode. Monitors in transparent mode can monitor pool members through firewalls. The default value is **disabled**.

◆ **username**
  Specifies the user name if the monitored target requires authentication. The default value is **none**.

**See also**

create, delete, edit, glob, gtm pool, list, modify, regex show, tmsh
imap

Configures an Internet Message Access Protocol (IMAP) monitor.

Module

gtm monitor

Syntax

Configure the imap component within the gtm monitor module using the following syntax.

Create/Modify

create imap [name]
modify imap [name]
  options:
    debug [no | yes]
    defaults-from [name]
    description [string]
    destination [ip address][port]
    folder [ [name] | none]
    ignore-down-response [enabled | disabled]
    interval [integer]
    password [none | [password] ]
    probe-timeout [integer]
    timeout [integer]
    transparent [enabled | disabled]
    username [ [name] | none]
edit imap [ [name] | [glob] | [regex] ] ... ]
  options:
    all-properties
    non-default properties

Display

list imap
list imap [ [name] | [glob] | [regex] ] ... ]
show running-config imap
show running-config imap [ [name] | [glob] | [regex] ] ... ]
  options:
    all-properties
    non-default-properties
    one-line
    partition
Delete

delte imap [name]

◆ Note

*You cannot delete default monitors.*

Description

You can use the `imap` component to configure a custom monitor, or you can use the default IMAP monitor that the Global Traffic Manager provides. This type of monitor verifies IMAP by attempting to open a specified mail folder on a server. This monitor is similar to the POP3 monitor.

Examples

Creates a monitor named `my imap` that inherits properties from the default IMAP monitor:

```
create imap my imap defaults-from imap
```

Displays the properties of all of the IMAP monitors:

```
list imap
```

Options

You can use these options with the `imap` component:

◆ **debug**

Specifies whether the monitor sends error messages and additional information to a log file created and labeled specifically for this monitor. You can use the log information to help diagnose and troubleshoot unsuccessful health checks. The default value is no.

The options are:

- **no**

  Specifies that the system does not redirect error messages and additional information related to this monitor.

- **yes**

  Specifies that the system redirects error messages and additional information to the

  `/var/log/<monitor_type>_<ip address>.<port>.log` file.

◆ **defaults-from**

Specifies the name of the monitor from which you want your custom monitor to inherit settings. The default value is `imap`.

◆ **description**

User-defined description.
◆ **destination**
   Specifies the IP address and service port of the resource that is the destination of this monitor. The default value is `*::*`.
   Possible values are:
   - `*::*`
     Specifies that the system marks a pool member **up** or **down** based on the response of the server at the IP address and port supplied by the pool member.
   - `*:port`
     Specifies that the system marks a pool member **up** or **down** based on the response of the server at the IP address supplied by the pool member and the port you specify.
   - `<IP address>:<port>`
     Specifies that the system marks a pool member **up** or **down** based on the response of the server at the IP address and port you specify.

◆ **folder**
   Specifies the name of the folder on the IMAP server that the monitor tries to open. The default value is `INBOX`.

◆ **glob**
   Displays the items that match the `glob` expression. For a description of `glob` expression syntax, see the `glob` man page.

◆ **ignore-down-response**
   Specifies whether the monitor ignores a down response from the system it is monitoring. The default value is `disabled`.

◆ **interval**
   Specifies the frequency at which the system issues the monitor check. The default value is 10 seconds.

◆ **name**
   Specifies a unique name for the component. This option is required for the commands **create**, **delete**, and **modify**.

◆ **partition**
   Displays the administrative partition in which the component resides.

◆ **password**
   Specifies the password if the monitored target requires authentication. The default value is `none`.

◆ **probe-timeout**
   Specifies the number of seconds after which the BIG-IP system times out the probe request to the BIG-IP system. The default value is 5 seconds.

◆ **regex**
   Displays the items that match the regular expression. The regular expression must be preceded by an at sign (`[@[regular expression]]`) to indicate that the identifier is a regular expression. For a description of regular expression syntax, see the `regex` man page.

◆ **timeout**
   Specifies the number of seconds the target has in which to respond to the monitor request. The default value is 31 seconds.
If the target responds within the set time period, it is considered **up**. If the target does not respond within the set time period, it is considered **down**. Also, if the target responds with a RESET packet, the system immediately flags the target as **down** without waiting for the timeout interval to expire.

- **transparent**
  Specifies whether the monitor operates in transparent mode. Monitors in transparent mode can monitor pool members through firewalls. The default value is **disabled**.

- **username**
  Specifies the user name if the monitored target requires authentication. The default value is **none**.

**See also**

`create`, `delete`, `edit`, `glob`, `gtm pool`, `list`, `modify`, `regex show`, `tmsh`
**Idap**


**Module**

`gtm monitor`

**Syntax**

Configure the `ldap` component within the `gtm monitor` module using the following syntax.

**Create/Modify**

```plaintext
create ldap [name]
modify ldap [name]
   options:
      base [none | [string] ]
      chase-referrals [ no | yes ]
      debug [no | yes]
      defaults-from [name]
      description [string]
      destination [ip address][port]
      filter [ [LDAP key] | none]
      ignore-down-response [enabled | disabled]
      interval [integer]
      mandatory-attributes [no | yes]
      password [none | [password] ]
      probe-timeout [integer]
      security [none | ssl | tls]
      timeout [integer]
      username [ [name] | none]

edit ldap [ [name] | [glob] | [regex] ] ... ]
   options:
      all-properties
      non-default properties
```

**Display**

```plaintext
list ldap
list ldap [ [name] | [glob] | [regex] ] ... ]
show running-config ldap
show running-config ldap [ [name] | [glob] | [regex] ] ... ]
```
options:
   all-properties
   non-default-properties
   one-line
   partition

Delete

delete ldap [name]

◆ Note
You cannot delete default monitors.

Description

You can use the `ldap` component to configure a custom monitor, or you can use the default LDAP monitor that the Global Traffic Manager provides. This type of monitor verifies the LDAP service by attempting to authenticate the specified user.

Examples

Creates a monitor named `my_ldap` that inherits properties from the default LDAP monitor:

```plaintext
create ldap my_ldap defaults-from ldap
```

Displays the properties of all of the LDAP monitors:

```plaintext
list ldap
```

Options

You can use these options with the `ldap` component:

◆ `base`
   Specifies the location in the LDAP tree from which the monitor starts the health check. A sample value is `dc=bigip-test,dc=net`. The default value is `none`.

◆ `chase-referrals`
   Specifies whether the monitor upon receipt of an LDAP referral entry chases that referral. The default value is `yes`.
   The options are:
   - `no`
     Specifies that the system will treat a referral entry as a normal entry and refrain from querying the remote LDAP server(s) pointed to by the referral entry.
• yes

◆ debug
Specifies whether the monitor sends error messages and additional information to a log file created and labeled specifically for this monitor. You can use the log information to help diagnose and troubleshoot unsuccessful health checks. The default value is no.

The options are:

• no
  Specifies that the system does not redirect error messages and additional information related to this monitor.

• yes
  Specifies that the system redirects error messages and additional information to the /var/log/<monitor_type>_<ip address>.<port>.log file.

◆ defaults-from
Specifies the name of the monitor from which you want your custom monitor to inherit settings. The default value is ldap.

◆ description
User-defined description.

◆ destination
Specifies the IP address and service port of the resource that is the destination of this monitor. The default value is *:*.

Possible values are:

• *:*  
  Specifies that the system marks a pool member up or down based on the response of the server at the IP address and port supplied by the pool member.

• *:port
  Specifies that the system marks a pool member up or down based on the response of the server at the IP address supplied by the pool member and the port you specify.

• <IP address>::<port>
  Specifies that the system marks a pool member up or down based on the response of the server at the IP address and port you specify.

◆ filter
Specifies an LDAP key for which the monitor searches. A sample value is objectclass=* . The default value is none.

◆ glob
Displays the items that match the glob expression. For a description of glob expression syntax, see the glob man page.

◆ ignore-down-response
Specifies whether the monitor ignores a down response from the system it is monitoring. The default value is disabled.

◆ interval
Specifies the frequency at which the system issues the monitor check. The default value is 10 seconds.
◆ **mandatory-attributes**
   Specifies whether the target must include attributes in its response to be considered **up**. The default value is **no**.
   The options are:
   - **no**
     Specifies that the system performs only a one-level search (based on the value of the **filter** option) and does not require that the target returns any attributes.
   - **yes**
     Specifies that the system performs a sub-tree search, and if the target returns no attributes, the target is considered **down**.

◆ **name**
   Specifies a unique name for the component. This option is required for the commands **create**, **delete**, and **modify**.

◆ **partition**
   Displays the administrative partition in which the component resides.

◆ **password**
   Specifies the password if the monitored target requires authentication. The default value is **none**.

◆ **probe-timeout**
   Specifies the number of seconds after which the BIG-IP system times out the probe request to the BIG-IP system. The default value is **5** seconds.

◆ **regex**
   Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. For a description of regular expression syntax, see the **regex** man page.

◆ **security**
   Specifies the secure communications protocol that the monitor uses to communicate with the target. The default value is **none**.
   The options are:
   - **none**
     Specifies that the system does not use a security protocol for communications with the target.
   - **ssl**
     Specifies that the system uses the SSL protocol for communications with the target.
   - **tls**
     Specifies that the system uses the TLS protocol for communications with the target.

◆ **timeout**
   Specifies the number of seconds the target has in which to respond to the monitor request. The default value is **31** seconds.
If the target responds within the set time period, it is considered **up**. If the target does not respond within the set time period, it is considered **down**. Also, if the target responds with a RESET packet, the system immediately flags the target as **down** without waiting for the timeout interval to expire.

- **username**
  Specifies the user name if the monitored target requires authentication. The default value is **none**.

**See also**

create, delete, edit, glob, gtm pool, list, modify, regex show, tmsh
mssql

Configures a Microsoft® Windows® Structured Query Language (MSSQL) monitor.

Module

**gtm monitor**

Syntax

Configure the mssql component within the gtm monitor module using the following syntax.

Create/Modify

```
create mssql [name]
modify mssql [name]
```

options:

- count [0 | 1]
- database [ [name] | none]
- debug [no | yes]
- defaults-from [name]
- description [string]
- destination [ip address][port]
- ignore-down-response [enabled | disabled]
- interval [integer]
- password [none | [password] ]
- probe-timeout [integer]
- recv [none | [string] ]
- recv-column [none | [string] ]
- recv-row [none | [string] ]
- send [none | [string] ]
- timeout [integer]
- username [ [name] | none]

```
edit mssql [ [name] | [glob] | [regex] ] ... ]
```

options:

- all-properties
- non-default properties

Display

```
list mssql
list mssql [ [name] | [glob] | [regex] ] ... ]
```
show running-config mssql
show running-config mssql [ [name] | [glob] | [regex] ] ... 

options:
   all-properties
   non-default-properties
   one-line
   partition

Delete

delete mssql [name]

◆ Note

You cannot delete default monitors.

Description

You can use the mssql component to configure a custom monitor, or you can use the default Microsoft Windows SQL monitor that the Global Traffic Manager provides. This type of monitor verifies Microsoft Windows SQL-based services.

Examples

Creates a monitor named my_mssql that inherits properties from the default MSSQL monitor:
create mssql my_mssql defaults-from mssql

Displays the properties of all of the MSSQL monitors:
list mssql

Options

You can use these options with the mssql component:

◆ count

Specifies the number of instances for which the system keeps a connection open. By default, when you assign instances of this monitor to a resource, the system keeps the connection to the database open. With this option you can assign multiple instances to the database while reducing the overhead that multiple open connections can cause.

A value of 0 (zero), the default, keeps the connection open for all instances. A value of 1 opens a new connection for each instance. Any other positive value keeps the connection open for that many instances; for example, a value of 5 keeps the connection open for five instances of this monitor.
◆ **database**
Specifies the name of the database with which the monitor attempts to communicate. The default value is none.

◆ **debug**
Specifies whether the monitor sends error messages and additional information to a log file created and labeled specifically for this monitor. You can use the log information to help diagnose and troubleshoot unsuccessful health checks. The default value is no.

The options are:

* no
  Specifies that the system does not redirect error messages and additional information related to this monitor.

* yes
  Specifies that the system redirects error messages and additional information to the
  /var/log/<monitor_type>_<ip address>_<port>.log file.

◆ **defaults-from**
Specifies the name of the monitor from which you want your custom monitor to inherit settings. The default value is mssql.

◆ **description**
User-defined description.

◆ **destination**
Specifies the IP address and service port of the resource that is the destination of this monitor. The default value is *:*.

Possible values are:

* *:* 
  Specifies that the system marks a pool member up or down based on the response of the server at the IP address and port supplied by the pool member.

* *:<port>
  Specifies that the system marks a pool member up or down based on the response of the server at the IP address supplied by the pool member and the port you specify.

* <IP address>:<port>
  Specifies that the system marks a pool member up or down based on the response of the server at the IP address and port you specify.

◆ **glob**
Displays the items that match the glob expression. For a description of glob expression syntax, see the glob man page.

◆ **ignore-down-response**
Specifies whether the monitor ignores a down response from the system it is monitoring. The default value is disabled.

◆ **interval**
Specifies the frequency at which the system issues the monitor check. The default value is 30 seconds.
◆ name
Specifies a unique name for the component. This option is required for the commands create, delete, and modify.

◆ partition
Displays the administrative partition in which the component resides.

◆ password
Specifies the password if the monitored target requires authentication. The default value is none.

◆ probe-timeout
Specifies the number of seconds after which the BIG-IP system times out the probe request to the BIG-IP system. The default value is 5 seconds.

◆ recv
Specifies the text string that the monitor looks for in the returned resource. The default value is none.

The most common receive expressions contain a text string that is included in a field in your database. If you do not specify a value for both the send and recv options, the monitor performs a simple service check and connect only.

◆ recv-column
Specifies the column in the database where the system expects the specified Receive String to be located. Specify this option only if you configure the send and recv options. The default value is none.

◆ recv-row
Specifies the row in the database where the system expects the specified Receive String to be located. Specify this option only if you configure the send and recv options. The default value is none.

◆ regex
Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. For a description of regular expression syntax, see the regex man page.

◆ send
Specifies the SQL query that the monitor sends to the target database, for example: SELECT count(*) FROM mytable.

If this value is null, then a valid connection suffices to determine that the service is up. In this case, the system does not need the recv option and ignores the option even if not null.

◆ timeout
Specifies the number of seconds the target has in which to respond to the monitor request. The default value is 91 seconds.

If the target responds within the set time period, it is considered up. If the target does not respond within the set time period, it is considered down. Also, if the target responds with a RESET packet, the system immediately flags the target as down without waiting for the timeout interval to expire.
- **username**
  Specifies the user name if the monitored target requires authentication. 
  The default value is **none**.

**See also**

create, delete, edit, glob, gtm pool, list, modify, regex show, tmsh
Chapter 21

mysql

Configures a MySQL® monitor.

Module

gtm monitor

Syntax

Configure the mysql component within the gtm monitor module using the following syntax.

Create/Modify

create mysql [name]
modify mysql [name]

options:
  count [0 | 1]
  database [ [name] | none]
  debug [no | yes]
  defaults-from [name]
  description [string]
  destination [ip address][port]
  ignore-down-response [enabled | disabled]
  interval [integer]
  password [none | [password] ]
  probe-timeout [integer]
  recv [none | [string] ]
  recv-column [none | [string] ]
  recv-row [none | [string] ]
  send [none | [string] ]
  timeout [integer]
  username [ [name] | none]

edit mysql [ [name] | [glob] | [regex] ] ... ]

options:
  all-properties
  non-default properties

Display

list mysql
list mysql [ [name] | [glob] | [regex] ] ... ]
show running-config mysql
show running-config mysql [ [name] | [glob] | [regex] ] ... ]
options:
  all-properties
  non-default-properties
  one-line
  partition

Delete

delete mysql [name]

◆ Note

You cannot delete default monitors.

Description

You can use the mysql component to configure a custom monitor, or you can use the default MySQL monitor that the Global Traffic Manager provides. This type of monitor verifies Microsoft Windows SQL-based services.

Examples

Creates a monitor named my_mysql that inherits properties from the default MySQL monitor:
create mysql my_mysql defaults-from mysql

Displays the properties of all of the MySQL monitors:
list mysql

Options

You can use these options with the mysql component:

◆ count
  Specifies the number of instances for which the system keeps a connection open. By default, when you assign instances of this monitor to a resource, the system keeps the connection to the database open. With this option you can assign multiple instances to the database while reducing the overhead that multiple open connections can cause.

  A value of 0 (zero), the default, keeps the connection open for all instances. A value of 1 opens a new connection for each instance. Any other positive value keeps the connection open for that many instances; for example, a value of 5 keeps the connection open for five instances of this monitor.
**database**
Specifies the name of the database with which the monitor attempts to communicate. The default value is **none**.

**debug**
Specifies whether the monitor sends error messages and additional information to a log file created and labeled specifically for this monitor. You can use the log information to help diagnose and troubleshoot unsuccessful health checks. The default value is **no**.

The options are:

- **no**
  Specifies that the system does not redirect error messages and additional information related to this monitor.

- **yes**
  Specifies that the system redirects error messages and additional information to the `/var/log/<monitor_type>_<ip address>_<port>.log` file.

**defaults-from**
Specifies the name of the monitor from which you want your custom monitor to inherit settings. The default value is **mssql**.

**description**
User-defined description.

**destination**
Specifies the IP address and service port of the resource that is the destination of this monitor. The default value is `*:*`.

Possible values are:

- ***:***
  Specifies that the system marks a pool member **up** or **down** based on the response of the server at the IP address and port supplied by the pool member.

- ***:port**
  Specifies that the system marks a pool member **up** or **down** based on the response of the server at the IP address supplied by the pool member and the port you specify.

- **<IP address>:\<port>**
  Specifies that the system marks a pool member **up** or **down** based on the response of the server at the IP address and port you specify.

**glob**
Displays the items that match the **glob** expression. For a description of **glob** expression syntax, see the **glob** man page.

**ignore-down-response**
Specifies whether the monitor ignores a down response from the system it is monitoring. The default value is **disabled**.

**interval**
Specifies the frequency at which the system issues the monitor check. The default value is 30 seconds.
◆ **name**
  Specifies a unique name for the component. This option is required for the commands `create`, `delete`, and `modify`.

◆ **partition**
  Displays the administrative partition in which the component resides.

◆ **password**
  Specifies the password if the monitored target requires authentication. The default value is `none`.

◆ **probe-timeout**
  Specifies the number of seconds after which the BIG-IP system times out the probe request to the BIG-IP system. The default value is 5 seconds.

◆ **recv**
  Specifies the text string that the monitor looks for in the returned resource. The default value is `none`.

  The most common receive expressions contain a text string that is included in a field in your database. If you do not specify a value for both the `send` and `recv` options, the monitor performs a simple service check and connect only.

◆ **recv-column**
  Specifies the column in the database where the system expects the specified Receive String to be located. Specify this option only if you configure the `send` and `recv` options. The default value is `none`.

◆ **recv-row**
  Specifies the row in the database where the system expects the specified Receive String to be located. Specify this option only if you configure the `send` and `recv` options. The default value is `none`.

◆ **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. For a description of regular expression syntax, see the `regex` man page.

◆ **send**
  Specifies the SQL query that the monitor sends to the target database, for example: `SELECT count(*) FROM mytable`.

  If this value is null, then a valid connection suffices to determine that the service is **up**. In this case, the system does not need the `recv` option and ignores the option even if not null.

◆ **timeout**
  Specifies the number of seconds the target has in which to respond to the monitor request. The default value is 91 seconds.

  If the target responds within the set time period, it is considered **up**. If the target does not respond within the set time period, it is considered **down**. Also, if the target responds with a RESET packet, the system immediately flags the target as **down** without waiting for the timeout interval to expire.
username
Specifies the user name if the monitored target requires authentication.
The default value is none.

See also
create, delete, edit, glob, gtm pool, list, modify, regex show, tmsh
nntp

Configures a Network News Transfer Protocol (NNTP) monitor.

Module

gtm monitor

Syntax

Configure the nntp component within the gtm monitor module using the following syntax.

Create/Modify

create nntp [name]
modify nntp [name]

options:
  debug [no | yes]
  defaults-from [name]
  description [string]
  destination [ip address][port]
  ignore-down-response [enabled | disabled]
  interval [integer]
  newsgroup [ [name] | none]
  password [none | [password] ]
  probe-timeout [integer]
  timeout [integer]
  username [ [name] | none]

edit nntp [ [name] | [glob] | [regex] ] ... ]

options:
  all-properties
  non-default properties

Display

list nntp
list nntp [ [name] | [glob] | [regex] ] ... ]
show running-config nntp
show running-config nntp [ [name] | [glob] | [regex] ] ... ]

options:
  all-properties
  non-default-properties
  one-line
  partition
Delete

```
delete nntp [name]
```

◆ Note

*You cannot delete default monitors.*

Description

You can use the `nntp` component to configure a custom monitor, or you can use the default NNTP monitor that the Global Traffic Manager provides. This type of monitor verifies the Usenet News protocol service by attempting to retrieve a newsgroup identification string from the server.

Examples

Creates a monitor named `my_nntp` that inherits properties from the default NNTP monitor:

```
create nntp my_nntp defaults-from nntp
```

Displays the properties of all of the NNTP monitors:

```
list nntp
```

Options

You can use these options with the `nntp` component:

◆ `debug`
  Specifies whether the monitor sends error messages and additional information to a log file created and labeled specifically for this monitor. You can use the log information to help diagnose and troubleshoot unsuccessful health checks. The default value is `no`.

  The options are:

  ◆ `no`
    Specifies that the system does not redirect error messages and additional information related to this monitor.

  ◆ `yes`
    Specifies that the system redirects error messages and additional information to the `/var/log/<monitor_type>_<ip address>_<port>.log` file.

◆ `defaults-from`
  Specifies the name of the monitor from which you want your custom monitor to inherit settings. The default value is `nntp`.

◆ `description`
  User-defined description.
◆ **destination**
  Specifies the IP address and service port of the resource that is the destination of this monitor. The default value is `*:*
  Possible values are:
  - `*:*
    Specifies that the system marks a pool member **up** or **down** based on the response of the server at the IP address and port supplied by the pool member.
  - `*:port`
    Specifies that the system marks a pool member **up** or **down** based on the response of the server at the IP address supplied by the pool member and the port you specify.
  - `<IP address>:<port>`
    Specifies that the system marks a pool member **up** or **down** based on the response of the server at the IP address and port you specify.

◆ **glob**
  Displays the items that match the **glob** expression. For a description of **glob** expression syntax, see the **glob** man page.

◆ **ignore-down-response**
  Specifies whether the monitor ignores a down response from the system it is monitoring. The default value is **disabled**.

◆ **interval**
  Specifies the frequency at which the system issues the monitor check. The default value is **30** seconds.

◆ **name**
  Specifies a unique name for the component. This option is required for the commands **create**, **delete**, and **modify**.

◆ **newsgroup**
  Specifies the name of the newsgroup that you are monitoring, for example **alt.car.mercedes**. The default value is **none**.

◆ **partition**
  Displays the administrative partition in which the component resides.

◆ **password**
  Specifies the password if the monitored target requires authentication. The default value is **none**.

◆ **probe-timeout**
  Specifies the number of seconds after which the BIG-IP system times out the probe request to the BIG-IP system. The default value is **5** seconds.

◆ **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (`@[regular expression]`) to indicate that the identifier is a regular expression. For a description of regular expression syntax, see the **regex** man page.
timeout
Specifies the number of seconds the target has in which to respond to the monitor request. The default value is 120 seconds.
If the target responds within the set time period, it is considered up. If the target does not respond within the set time period, it is considered down. Also, if the target responds with a RESET packet, the system immediately flags the target as down without waiting for the timeout interval to expire.

username
Specifies the user name if the monitored target requires authentication. The default value is none.

See also
create, delete, edit, glob, gtm pool, list, modify, regex show, tmsh
oracle

Configures an Oracle® monitor.

Module

gtm monitor

Syntax

Configure the oracle component within the gtm monitor module using the following syntax.

Create/Modify

```
create oracle [name]
modify oracle [name]
```

options:
- count [0 | 1]
- database [ [name] | none]
- debug [no | yes]
- defaults-from [name]
- description [string]
- destination [ip address][port]
- ignore-down-response [enabled | disabled]
- interval [integer]
- password [none | [password] ]
- probe-timeout [integer]
- recv [none | [string] ]
- recv-column [none | [string] ]
- recv-row [none | [string] ]
- send [none | [string] ]
- timeout [integer]
- username [ [name] | none]

edit oracle [ [name] | [glob] | [regex] ] ... 

options:
- all-properties
- non-default properties

Display

```
list oracle
list oracle [ [name] | [glob] | [regex] ] ... 
show running-config oracle
```
show running-config oracle [ [name] | [glob] | [regex] ] ... }

options:
  all-properties
  non-default-properties
  one-line
  partition

Delete

delete oracle [name]

◆ Note

You cannot delete default monitors.

Description

You can use the oracle component to configure a custom monitor, or you can use the default Oracle monitor that the Global Traffic Manager provides. This type of monitor verifies services based on Oracle by attempting to perform an Oracle logon to a service.

Examples

Creates a monitor named my_oracle that inherits properties from the default Oracle monitor:

create oracle my_oracle defaults-from oracle

Displays the properties of all of the Oracle monitors:

list oracle

Options

You can use these options with the oracle component:

◆ count

  Specifies the number of instances for which the system keeps a connection open. By default, when you assign instances of this monitor to a resource, the system keeps the connection to the database open. With this option you can assign multiple instances to the database while reducing the overhead that multiple open connections can cause.

  A value of 0 (zero), the default, keeps the connection open for all instances. A value of 1 opens a new connection for each instance. Any other positive value keeps the connection open for that many instances; for example, a value of 5 keeps the connection open for five instances of this monitor.
- **database**
  Specifies the name of the database with which the monitor attempts to communicate. The default value is **none**.

- **debug**
  Specifies whether the monitor sends error messages and additional information to a log file created and labeled specifically for this monitor. You can use the log information to help diagnose and troubleshoot unsuccessful health checks. The default value is **no**.
  
  The options are:
  
  - **no**
    Specifies that the system does not redirect error messages and additional information related to this monitor.
  
  - **yes**
    Specifies that the system redirects error messages and additional information to the `/var/log/<monitor_type>_<ip address>_<port>.log` file.

- **defaults-from**
  Specifies the name of the monitor from which you want your custom monitor to inherit settings. The default value is **oracle**.

- **description**
  User-defined description.

- **destination**
  Specifies the IP address and service port of the resource that is the destination of this monitor. The default value is `*:*`.
  
  Possible values are:
  
  - `*:*`
    Specifies that the system marks a pool member **up** or **down** based on the response of the server at the IP address and port supplied by the pool member.
  
  - `*:<port>`
    Specifies that the system marks a pool member **up** or **down** based on the response of the server at the IP address supplied by the pool member and the port you specify.
  
  - `<IP address>:<port>`
    Specifies that the system marks a pool member **up** or **down** based on the response of the server at the IP address and port you specify.

- **glob**
  Displays the items that match the **glob** expression. For a description of **glob** expression syntax, see the **glob** man page.

- **ignore-down-response**
  Specifies whether the monitor ignores a down response from the system it is monitoring. The default value is **disabled**.

- **interval**
  Specifies the frequency at which the system issues the monitor check. The default value is **30** seconds.
◆ **name**
   Specifies a unique name for the component. This option is required for the commands **create**, **delete**, and **modify**.

◆ **partition**
   Displays the administrative partition in which the component resides.

◆ **password**
   Specifies the password if the monitored target requires authentication. The default value is **none**.

◆ **probe-timeout**
   Specifies the number of seconds after which the BIG-IP system times out the probe request to the BIG-IP system. The default value is 5 seconds.

◆ **recv**
   Specifies the text string that the monitor looks for in the returned resource. The default value is **none**.
   The most common receive expressions contain a text string that is included in a field in your database. If you do not specify a value for both the **send** and **recv** options, the monitor performs a simple service check and connect only.

◆ **recv-column**
   Specifies the column in the database where the system expects the specified Receive String to be located. Specify this option only if you configure the **send** and **recv** options. The default value is **none**.

◆ **recv-row**
   Specifies the row in the database where the system expects the specified Receive String to be located. Specify this option only if you configure the **send** and **recv** options. The default value is **none**.

◆ **regex**
   Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. For a description of regular expression syntax, see the **regex** man page.

◆ **send**
   Specifies the SQL query that the monitor sends to the target database, for example: `SELECT count(*) FROM mytable`.
   If this value is null, then a valid connection suffices to determine that the service is **up**. In this case, the system does not need the **recv** option and ignores the option even if not null.

◆ **timeout**
   Specifies the number of seconds the target has in which to respond to the monitor request. The default value is 91 seconds.
   If the target responds within the set time period, it is considered **up**. If the target does not respond within the set time period, it is considered **down**. Also, if the target responds with a RESET packet, the system immediately flags the target as **down** without waiting for the timeout interval to expire.
• **username**
  Specifies the user name if the monitored target requires authentication.
  The default value is **none**.

See also

create, delete, edit, glob, gtm pool, list, modify, regex show, tmsh
**pop3**

Configures a Post Office Protocol version 3 (POP3) monitor.

**Module**

gtm monitor

**Syntax**

Configure the pop3 component within the gtm monitor module using the following syntax.

**Create/Modify**

```
create pop3 [name]
modify pop3 [name]
```

options:
- debug [no | yes]
- defaults-from [name]
- description [string]
- destination [ip address][port]
- ignore-down-response [enabled | disabled]
- interval [integer]
- password [none | [password] ]
- probe-timeout [integer]
- timeout [integer]
- username [ [name] | none]

```
edit pop3 [ [name] | [glob] | [regex] ] ... ]
edit pop3 [ [name] | [glob] | [regex] ] ... ]
```

options:
- all-properties
- non-default properties

**Display**

```
list pop3
list pop3 [ [name] | [glob] | [regex] ] ... ]
```

```
show running-config pop3
```

```
show running-config pop3 [ [name] | [glob] | [regex] ] ... ]
```

options:
- all-properties
- non-default-properties
- one-line
- partition
Delete

delete pop3 [name]

◆ Note

You cannot delete default monitors.

Description

You can use the pop3 component to configure a custom monitor, or you can use the default POP3 monitor that the Global Traffic Manager provides. This type of monitor verifies the POP3 service by attempting to connect to a pool, pool member, or virtual server; log on as the specified user; and log off.

Examples

Creates a monitor named my_pop3 that inherits properties from the default POP3 monitor:

create pop3 my_pop3 defaults-from pop3

Displays the properties of all of the POP3 monitors:

list pop3

Options

You can use these options with the pop3 component:

◆ debug
  Specifies whether the monitor sends error messages and additional information to a log file created and labeled specifically for this monitor. You can use the log information to help diagnose and troubleshoot unsuccessful health checks. The default value is no.

  The options are:
  • no
    Specifies that the system does not redirect error messages and additional information related to this monitor.

  • yes
    Specifies that the system redirects error messages and additional information to the /var/log/<monitor_type>_<ip address>_<port>.log file.

◆ defaults-from
  Specifies the name of the monitor from which you want your custom monitor to inherit settings. The default value is pop3.

◆ description
  User-defined description.
◆ **destination**
   Specifies the IP address and service port of the resource that is the destination of this monitor. The default value is `*:*`.
   Possible values are:
   - `*:*`
     Specifies that the system marks a pool member **up or down** based on the response of the server at the IP address and port supplied by the pool member.
   - `*:port`
     Specifies that the system marks a pool member **up or down** based on the response of the server at the IP address supplied by the pool member and the port you specify.
   - `<IP address>:<port>`
     Specifies that the system marks a pool member **up or down** based on the response of the server at the IP address and port you specify.

◆ **glob**
   Displays the items that match the **glob** expression. For a description of **glob** expression syntax, see the **glob** man page.

◆ **ignore-down-response**
   Specifies whether the monitor ignores a down response from the system it is monitoring. The default value is **disabled**.

◆ **interval**
   Specifies the frequency at which the system issues the monitor check. The default value is **30** seconds.

◆ **name**
   Specifies a unique name for the component. This option is required for the commands **create**, **delete**, and **modify**.

◆ **partition**
   Displays the administrative partition in which the component resides.

◆ **password**
   Specifies the password if the monitored target requires authentication. The default value is **none**.

◆ **probe-timeout**
   Specifies the number of seconds after which the BIG-IP system times out the probe request to the BIG-IP system. The default value is **5** seconds.

◆ **regex**
   Displays the items that match the regular expression. The regular expression must be preceded by an at sign (`@[regular expression]`) to indicate that the identifier is a regular expression. For a description of regular expression syntax, see the **regex** man page.

◆ **timeout**
   Specifies the number of seconds the target has in which to respond to the monitor request. The default value is **120** seconds.
If the target responds within the set time period, it is considered **up**. If the target does not respond within the set time period, it is considered **down**. Also, if the target responds with a RESET packet, the system immediately flags the target as **down** without waiting for the timeout interval to expire.

* **username**
  Specifies the user name if the monitored target requires authentication. The default value is **none**.

**See also**

create, delete, edit, glob, gtm pool, list, modify, regex show, tmsh
**postgreSQL**

Configures a PostgreSQl® monitor.

**Module**

`gtm monitor`

**Syntax**

Configure the `postgreSQL` component within the `gtm monitor` module using the following syntax.

**Create/Modify**

```plaintext
create postgreSQL [name]
modify postgreSQL [name]
```

Options:

- `count [0 | 1]`
- `database [name | none]`
- `debug [no | yes]`
- `defaults-from [name]`
- `description [string]`
- `destination [ip address][port]`
- `ignore-down-response [enabled | disabled]`
- `interval [integer]`
- `password [none | [password]]`
- `probe-timeout [integer]`
- `recv [none | [string]]`
- `recv-column [none | [string]]`
- `recv-row [none | [string]]`
- `send [none | [string]]`
- `timeout [integer]`
- `username [name | none]`

**edit postgreSQL [ [name] | [glob] | [regex] ] ... ]**

Options:

- `all-properties`
- `non-default properties`

**Display**

```plaintext
list postgreSQL
list postgreSQL [ [name] | [glob] | [regex] ] ... ]
show running-config postgreSQL
```
show running-config postgresql [ [name] | [glob] | [regex] ] ... ]
  options:
    all-properties
    non-default-properties
    one-line
    partition

Delete

delete postgresql [name]

◆ Note

You cannot delete default monitors.

Description

You can use the postgresql component to configure a custom monitor, or you can use the default PostgreSQL monitor that the Global Traffic Manager provides. This type of monitor verifies Microsoft Windows SQL-based services.

Examples

Creates a monitor named my_postgresql that inherits properties from the default PostgreSQL monitor:

create postgresql my_postgresql defaults-from postgresql

Displays the properties of all of the PostgreSQL monitors:

list postgresql

Options

You can use these options with the mysql component:

◆ count

Specifies the number of instances for which the system keeps a connection open. By default, when you assign instances of this monitor to a resource, the system keeps the connection to the database open. With this option you can assign multiple instances to the database while reducing the overhead that multiple open connections can cause.

A value of 0 (zero), the default, keeps the connection open for all instances. A value of 1 opens a new connection for each instance. Any other positive value keeps the connection open for that many instances; for example, a value of 5 keeps the connection open for five instances of this monitor.
database
Specifies the name of the database with which the monitor attempts to communicate. The default value is none.

debug
Specifies whether the monitor sends error messages and additional information to a log file created and labeled specifically for this monitor. You can use the log information to help diagnose and troubleshoot unsuccessful health checks. The default value is no.

The options are:

- no
  Specifies that the system does not redirect error messages and additional information related to this monitor.

- yes
  Specifies that the system redirects error messages and additional information to the /var/log/<monitor_type>_<ip address>_<port>.log file.

defaults-from
Specifies the name of the monitor from which you want your custom monitor to inherit settings. The default value is mssql.

description
User-defined description.

destination
Specifies the IP address and service port of the resource that is the destination of this monitor. The default value is *:*.

Possible values are:

- *:*  
  Specifies that the system marks a pool member up or down based on the response of the server at the IP address and port supplied by the pool member.

- *:port
  Specifies that the system marks a pool member up or down based on the response of the server at the IP address supplied by the pool member and the port you specify.

- <IP address>:<port>
  Specifies that the system marks a pool member up or down based on the response of the server at the IP address and port you specify.

glob
Displays the items that match the glob expression. For a description of glob expression syntax, see the glob man page.

glob-expression
Specifies whether the monitor ignores a down response from the system it is monitoring. The default value is disabled.

interval
Specifies the frequency at which the system issues the monitor check. The default value is 30 seconds.
◆ **name**
   Specifies a unique name for the component. This option is required for the commands `create`, `delete`, and `modify`.

◆ **partition**
   Displays the administrative partition in which the component resides.

◆ **password**
   Specifies the password if the monitored target requires authentication. The default value is `none`.

◆ **probe-timeout**
   Specifies the number of seconds after which the BIG-IP system times out the probe request to the BIG-IP system. The default value is 5 seconds.

◆ **recv**
   Specifies the text string that the monitor looks for in the returned resource. The default value is `none`.
   The most common receive expressions contain a text string that is included in a field in your database. If you do not specify a value for both the `send` and `recv` options, the monitor performs a simple service check and connect only.

◆ **recv-column**
   Specifies the column in the database where the system expects the specified Receive String to be located. Specify this option only if you configure the `send` and `recv` options. The default value is `none`.

◆ **recv-row**
   Specifies the row in the database where the system expects the specified Receive String to be located. Specify this option only if you configure the `send` and `recv` options. The default value is `none`.

◆ **regex**
   Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. For a description of regular expression syntax, see the `regex` man page.

◆ **send**
   Specifies the SQL query that the monitor sends to the target database, for example: `SELECT count(*) FROM mytable`.
   If this value is null, then a valid connection suffices to determine that the service is `up`. In this case, the system does not need the `recv` option and ignores the option even if not null.

◆ **timeout**
   Specifies the number of seconds the target has in which to respond to the monitor request. The default value is 91 seconds.
   If the target responds within the set time period, it is considered `up`. If the target does not respond within the set time period, it is considered `down`. Also, if the target responds with a RESET packet, the system immediately flags the target as `down` without waiting for the timeout interval to expire.
username
Specifies the user name if the monitored target requires authentication.
The default value is none.

See also
create, delete, edit, glob, gtm pool, list, modify, regex show, tmsh
radius

Configures a Remote Access Dial-in User Service (RADIUS) monitor.

Module

gtm monitor

Syntax

Configure the radius component within the gtm monitor module using the following syntax.

Create/Modify

create radius [name]
modify radius [name]

options:
  debug [no | yes]
  defaults-from [name]
  description [string]
  destination [ip address][port]
  ignore-down-response [enabled | disabled]
  interval [integer]
  nas-ip-address [ [ip address] | none]
  password [none | [password] ]
  probe-timeout [integer]
  secret [none | [secret] ]
  timeout [integer]
  username [ [name] | none]

edit radius [ [name] | [glob] | [regex] ] ... 

options:
  all-properties
  non-default properties

Display

list radius
list radius [ [name] | [glob] | [regex] ] ... 
show running-config radius
show running-config radius [ [name] | [glob] | [regex] ] ... 

options:
  all-properties
  non-default-properties
  one-line
  partition
Delete

delete radius [name]

◆ Note

You cannot delete default monitors.

Description

You can use the radius component to configure a custom monitor, or you can use the default RADIUS monitor that the Global Traffic Manager provides. This type of monitor verifies the RADIUS service by attempting to authenticate the specified user.

Examples

Creates a monitor named my_radius that inherits properties from the default RADIUS monitor:

create radius my_radius defaults-from radius

Displays the properties of all of the POP3 monitors:

list radius

Options

You can use these options with the radius component:

◆ debug
  Specifies whether the monitor sends error messages and additional information to a log file created and labeled specifically for this monitor. You can use the log information to help diagnose and troubleshoot unsuccessful health checks. The default value is no.

  The options are:
  • no
  Specifies that the system does not redirect error messages and additional information related to this monitor.
  • yes
  Specifies that the system redirects error messages and additional information to the
  /var/log/<monitor_type>_<ip address>_<port>.log file.

◆ defaults-from
  Specifies the name of the monitor from which you want your custom monitor to inherit settings. The default value is radius.

◆ description
  User-defined description.
◆ destination
  Specifies the IP address and service port of the resource that is the
destination of this monitor. The default value is *:*.

  Possible values are:
  • *:*  
    Specifies that the system marks a pool member up or down based on
    the response of the server at the IP address and port supplied by the
    pool member.
  • *:port  
    Specifies that the system marks a pool member up or down based on
    the response of the server at the IP address supplied by the pool
    member and the port you specify.
  • <IP address>:<port>  
    Specifies that the system marks a pool member up or down based on
    the response of the server at the IP address and port you specify.

◆ glob
  Displays the items that match the glob expression. For a description of
  glob expression syntax, see the glob man page.

◆ ignore-down-response
  Specifies whether the monitor ignores a down response from the system
  it is monitoring. The default value is disabled.

◆ interval
  Specifies the frequency at which the system issues the monitor check.
The default value is 30 seconds.

◆ name
  Specifies a unique name for the component. This option is required for
  the commands create, delete, and modify.

◆ nas-ip-address
  Specifies the network access server IP address that the system uses to
  identify itself to the RADIUS server. Using this option, multiple BIG-IP
  systems can appear as a single network access device to the RADIUS
  server. The default value is none.

◆ partition
  Displays the administrative partition in which the component resides.

◆ password
  Specifies the password if the monitored target requires authentication.
The default value is none.

◆ probe-timeout
  Specifies the number of seconds after which the BIG-IP system times out
  the probe request to the BIG-IP system. The default value is 5 seconds.

◆ regex
  Displays the items that match the regular expression. The regular
  expression must be preceded by an at sign (@[regular expression]) to
  indicate that the identifier is a regular expression. For a description of
  regular expression syntax, see the regex man page.
◆ secret
  Specifies the secret the monitor needs to communicate with the resource. The default value is none.

◆ timeout
  Specifies the number of seconds the target has in which to respond to the monitor request. The default value is 31 seconds.
  If the target responds within the set time period, it is considered up. If the target does not respond within the set time period, it is considered down. Also, if the target responds with a RESET packet, the system immediately flags the target as down without waiting for the timeout interval to expire.

◆ username
  Specifies the user name if the monitored target requires authentication. The default value is none.

See also

create, delete, edit, glob, gtm pool, list, modify, regex show, tmsh
radius-accounting


Module

gtm monitor

Syntax

Configure the radius-accounting component within the gtm monitor module using the following syntax.

Create/Modify

create radius-accounting [name]
modify radius-accounting [name]
  options:
    check-until-up [disabled | enabled]
    debug [no | yes]
    defaults-from [ [name] | none]
    destination [ip address]
    interval [integer]
    manual-resume [disabled | enabled]
    nas-ip-address [ip address]
    secret [string]
    time-until-up [integer]
    timeout [integer]
    username [none | [string] ]

edit radius-accounting [ [ [name] | [glob] | [regex] ] ... ]
  options:
    all-properties
    non-default-properties

Display

list radius-accounting
list radius-accounting [ [ [name] | [glob] | [regex] ] ... ]
show running-config radius-accounting
show running-config radius-accounting [ [ [name] | [glob] | [regex] ] ... ]
  options:
    all-properties
    non-default-properties
    one-line
    partition
Delete

```
delete radius-accounting [name]
```

◆ Note

You cannot delete default monitors.

Description

You can use the `radius-accounting` component to configure a custom monitor, or you can use the default RADIUS accounting monitor that the Global Traffic Manager provides.

Examples

Creates a monitor named `my_radius_acct` that inherits properties from the default RADIUS accounting monitor.

```
create radius my_radius_acct defaults-from radius_accounting
```

Displays the properties of all of the RADIUS accounting monitors:

```
list radius-accounting
```

Options

You can use these options with the `radius` component:

◆ **check-until-up**
When enabled, specifies that when an active and passive (inband) monitor are combined in an AND type of rule, the active monitor performs health checks only when the pool member is `down`, or until the pool member is marked as `up`. When the passive monitor marks the pool member `down`, the active monitor resumes health checks.

The default value is `disabled`.

◆ **debug**
Specifies whether the monitor sends error messages and additional information to a log file created and labeled specifically for this monitor. You can use the log information to help diagnose and troubleshoot unsuccessful health checks. The default value is `no`.

The options are:

- **no**
  Specifies that the system does not redirect error messages and additional information related to this monitor.

- **yes**
  Specifies that the system redirects error messages and additional information to the

  `/var/log/<monitor_type>_<ip address>_<port>_.log` file.
◆ **defaults-from**
   Specifies the name of the monitor from which you want your custom monitor to inherit settings. The default value is **radius**.

◆ **description**
   User-defined description.

◆ **destination**
   Specifies the IP address and service port of the resource that is the destination of this monitor. The default value is **:***.
   Possible values are:
   - **:***
     Specifies that the system marks a pool member **up** or **down** based on the response of the server at the IP address and port supplied by the pool member.
   - **:*:port**
     Specifies that the system marks a pool member **up** or **down** based on the response of the server at the IP address supplied by the pool member and the port you specify.
   - **<IP address>:<port>**
     Specifies that the system marks a pool member **up** or **down** based on the response of the server at the IP address and port you specify.

◆ **glob**
   Displays the items that match the **glob** expression. For a description of **glob** expression syntax, see the **glob** man page.

◆ **interval**
   Specifies the frequency at which the system issues the monitor check. The default value is **10** seconds.

◆ **manual-resume**
   Specifies whether the system automatically changes the status of a resource to **up** at the next successful monitor check. The default value of the **manual-resume** option is **disabled**.
   If you set the **manual-resume** option to **enabled**, you must manually mark the resource as **up** before the system can use it for load balancing connections.

◆ **name**
   Specifies a unique name for the component. This option is required for the commands **create**, **delete**, and **modify**.

◆ **nas-ip-address**
   Specifies the network access server IP address that the system uses to identify itself to the RADIUS server. With this option, multiple BIG-IP systems can appear as a single network access device to the RADIUS server. The default value is **none**.

◆ **partition**
   Displays the administrative partition in which the component resides.
◆ regex
Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. For a description of regular expression syntax, see the regex man page.

◆ secret
Specifies the secret the monitor must use when contacting the resource. The default value is none.

◆ time-until-up
Specifies the amount of time in seconds after the first successful response before a node is marked up. A value of 0 (zero) causes a node to be marked up immediately after a valid response is received from the node. The default value is 0 (zero).

◆ timeout
Specifies the number of seconds the target has in which to respond to the monitor request. The default value is 31 seconds.

If the target responds within the set time period, it is considered up. If the target does not respond within the set time period, it is considered down. Also, if the target responds with a RESET packet, the system immediately flags the target as down without waiting for the timeout interval to expire.

◆ username
Specifies the user name if the monitored target requires authentication. The default value is none.

See also

create, delete, edit, glob, list, modify, regex, show, tmsh
real-server

Configures a RealServer® monitor.

Module

gtm monitor

Syntax

Configure the real-server component within the gtm monitor module using the following syntax.

Create/Modify

create real-server [name]
modify real-server [name]

options:
  defaults-from [name]
description [string]
ignore-down-response [enabled | disabled]
interval [integer]
metrics [metrics | none]
probe-timeout [integer]
timeout [integer]

edit real-server [ [name] | [glob] | [regex] ] ...

options:
  all-properties
  non-default properties

Display

list real-server
list real-server [ [name] | [glob] | [regex] ] ...
show running-config real-server
show running-config real-server [ [name] | [glob] | [regex] ] ...

options:
  agent
  all-properties
  command
  method
  non-default-properties
  one-line
  partition
Delete

```
delete real-server [name]
```

◆ Note

*You cannot delete default monitors.*

Description

You can use the `real-server` component to configure a custom monitor, or you can use the default RealServer monitor that the Global Traffic Manager provides. This type of monitor checks the performance of a pool, pool member, or virtual server that is running the RealServer data collection agent, and then dynamically load balances traffic accordingly.

Examples

Creates a monitor named `my_real-server` that inherits properties from the default RealServer monitor:

```
create real-server my_real-server defaults-from real_server
```

Displays the properties of all of the RealServer monitors:

```
list real-server
```

Options

You can use these options with the `real-server` component:

◆ `agent`
  Displays the agent for the monitor. The default agent is Mozilla/4.0 (compatible: MSIE 5.0; Windows NT). You cannot modify the agent.

◆ `command`
  Displays the command that the system uses to obtain the metrics from the resource. See the documentation for this resource for information on available commands.

◆ `defaults-from`
  Specifies the name of the monitor from which you want your custom monitor to inherit settings. The default value is `real_server`.

◆ `glob`
  Displays the items that match the `glob` expression. For a description of `glob` expression syntax, see the `glob` man page.

◆ `ignore-down-response`
  Specifies whether the monitor ignores a down response from the system it is monitoring. The default value is `disabled`. 
gtm monitor Module Components

- **interval**
  Specifies the frequency at which the system issues the monitor check.
  The default value is 30 seconds.

- **name**
  Specifies a unique name for the component. This option is required for
  the commands create, delete, and modify.

- **method**
  Displays the GET method. You cannot modify the method.

- **metrics**
  Specifies the performance metrics that the commands collect from the
  target. The default value is `ServerBandwidth:1.5, CPUPercentUsage, MemoryUsage, TotalClientCount`.

- **partition**
  Displays the administrative partition in which the component resides.

- **probe-timeout**
  Specifies the number of seconds after which the BIG-IP system times out
  the probe request to the BIG-IP system. The default value is 5 seconds.

- **regex**
  Displays the items that match the regular expression. The regular
  expression must be preceded by an at sign (@[regular expression]) to
  indicate that the identifier is a regular expression. For a description
  of regular expression syntax, see the regex man page.

- **timeout**
  Specifies the number of seconds the target has in which to respond to the
  monitor request. The default value is 120 seconds.
  If the target responds within the set time period, it is considered up.
  If the target does not respond within the set time period, it is considered down.
  Also, if the target responds with a RESET packet, the system
  immediately flags the target as down without waiting for the timeout
  interval to expire.

**See also**

create, delete, edit, glob, gtm pool, gtm server, list, ltm node, modify,
regex, show, tmsh
scripted

Configures a Scripted monitor.

Module

gtm monitor

Syntax

Configure the scripted component within the gtm monitor module using the following syntax.

Create/Modify

create scripted [name]
modify scripted [name]

options:
  debug [no | yes]
  defaults-from [name]
  description [string]
  destination [ip address] [port]
  filename [ [filename] | none]
  ignore-down-response [enabled | disabled]
  interval [integer]
  probe-timeout [integer]
  timeout [integer]

edit scripted [ [name] | [glob] | [regex] ] ... ]

options:
  all-properties
  non-default properties

Display

list scripted
list scripted [ [name] | [glob] | [regex] ] ... ]
show running-config scripted
show running-config scripted [ [name] | [glob] | [regex] ] ... ]

options:
  all-properties
  non-default-properties
  one-line
  partition
Delete

\texttt{delete scripted [name]}

\noindent\textbf{\textcolor{red}{\textbullet\ Note}}

\emph{You cannot delete default monitors.}

Description

You can use the \texttt{scripted} component to configure a custom monitor, or you can use the default Scripted monitor that the Global Traffic Manager provides.

Examples

Creates a monitor named \texttt{my\_scripted} that inherits properties from the default Scripted monitor:

\texttt{create scripted my\_scripted defaults-from scripted}

Displays the properties of all of the Scripted monitors:

\texttt{list scripted}

Options

You can use these options with the \texttt{scripted} component:

\noindent\textbf{\textcolor{red}{\textbullet\ debug}}

Specifies whether the monitor sends error messages and additional information to a log file created and labeled specifically for this monitor. You can use the log information to help diagnose and troubleshoot unsuccessful health checks. The default value is \texttt{no}.

The options are:

\noindent\textbf{\textcolor{red}{\textbullet\ no}}

Specifies that the system does not redirect error messages and additional information related to this monitor.

\noindent\textbf{\textcolor{red}{\textbullet\ yes}}

Specifies that the system redirects error messages and additional information to the \texttt{/var/log/<monitor\_type>_<ip\ address>_<port>.log} file.

\noindent\textbf{\textcolor{red}{\textbullet\ defaults-from}}

Specifies the name of the monitor from which you want your custom monitor to inherit settings. The default value is \texttt{scripted}.

\noindent\textbf{\textcolor{red}{\textbullet\ description}}

User-defined description.
◆ **destination**
   Specifies the IP address and service port of the resource that is the destination of this monitor. The default value is `*:*`.
   Possible values are:
   - `*:*`
     Specifies that the system marks a pool member **up** or **down** based on the response of the server at the IP address and port supplied by the pool member.
   - `*:port`
     Specifies that the system marks a pool member **up** or **down** based on the response of the server at the IP address supplied by the pool member and the port you specify.
   - `<IP address>:<port>`
     Specifies that the system marks a pool member **up** or **down** based on the response of the server at the IP address and port you specify.

◆ **filename**
   Specifies the name of a file in the `/config/eav/` directory on the system. The user-created file contains the send and expect data that the monitor uses for the monitor check. The default value is `none`.

◆ **glob**
   Displays the items that match the **glob** expression. For a description of **glob** expression syntax, see the **glob** man page.

◆ **ignore-down-response**
   Specifies whether the monitor ignores a down response from the system it is monitoring. The default value is `disabled`.

◆ **interval**
   Specifies the frequency at which the system issues the monitor check. The default value is **10** seconds.

◆ **name**
   Specifies a unique name for the component. This option is required for the commands **create**, **delete**, and **modify**.

◆ **partition**
   Displays the administrative partition in which the component resides.

◆ **probe-timeout**
   Specifies the number of seconds after which the BIG-IP system times out the probe request to the BIG-IP system. The default value is **5** seconds.

◆ **regex**
   Displays the items that match the regular expression. The regular expression must be preceded by an at sign (`@[regular expression]`) to indicate that the identifier is a regular expression. For a description of regular expression syntax, see the **regex** man page.
timeout

Specifies the number of seconds the target has in which to respond to the monitor request. The default value is 31 seconds.

If the target responds within the set time period, it is considered **up**. If the target does not respond within the set time period, it is considered **down**. Also, if the target responds with a RESET packet, the system immediately flags the target as **down** without waiting for the timeout interval to expire.

See also

create, delete, edit, glob, gtm pool, list, modify, regex show, tmsh
**sip**

Configures a Session Initiation Protocol (SIP) monitor.

**Module**

gtm monitor

**Syntax**

Configure the **sip** component within the **gtm monitor** module using the following syntax.

**Create/Modify**

```plaintext
create sip [name]
modify sip [name]
  options:
    cert [ [cert list] | none]
    cipherlist [list]
    compatibility [enabled | disabled]
    debug [no | yes]
    defaults-from [name]
    description [string]
    destination [ip address][port]
    filter [any | none | status]
    filter-neg [any | none | status]
    headers [ [new line separated headers] | none]
    ignore-down-response [enabled | disabled]
    interval [integer]
    key [ [key] | none]
    mode [sips | tcp | tls | udp]
    probe-timeout [integer]
    request [none | [string] ]
    username [ [name] | none]
```

```plaintext
edit sip [ [name] | [glob] | [regex] ] ...]
  options:
    all-properties
    non-default properties
```

**Display**

```plaintext
list sip
list sip [ [name] | [glob] | [regex] ] ... ]
```
show running-config sip
show running-config sip [ [name] | [glob] | [regex] ] ... ]

options:
  all-properties
  non-default-properties
  one-line
  partition

Delete

delete sip [name]

◆ Note

You cannot delete default monitors.

Description

You can use the \texttt{sip} component to configure a custom monitor, or you can use the default SIP monitor that the Global Traffic Manager provides. This type of monitor checks the status of SIP Call-ID services on a device. The SIP protocol enables real-time messaging, voice, data, and video.

Examples

Creates a monitor named \texttt{my\_sip} that inherits properties from the default SIP monitor:

\texttt{create sip my\_sip defaults-from sip}

Displays the properties of all of the SIP monitors:

\texttt{list sip}

Options

You can use these options with the \texttt{sip} component:

- \texttt{cert}
  Specifies a fully-qualified path for a client certificate that the monitor sends to the target SSL server. The default value is \texttt{none}.

- \texttt{cipherlist}
  Specifies the list of ciphers for this monitor. The default value is \texttt{none}.

- \texttt{compatibility}
  Specifies, when enabled, that the SSL options setting (in OpenSSL) is set to \texttt{ALL}. The default value is \texttt{enabled}. 
◆ debug
Specifies whether the monitor sends error messages and additional information to a log file created and labeled specifically for this monitor. You can use the log information to help diagnose and troubleshoot unsuccessful health checks. The default value is **no**.

The options are:

- **no**
  Specifies that the system does not redirect error messages and additional information related to this monitor.

- **yes**
  Specifies that the system redirects error messages and additional information to the `/var/log/<monitor_type>_<ip address>,<port>.log` file.

◆ defaults-from
Specifies the name of the monitor from which you want your custom monitor to inherit settings. The default value is **sip**.

◆ description
User-defined description.

◆ destination
Specifies the IP address and service port of the resource that is the destination of this monitor. The default value is `*:*`.

Possible values are:

- ***:***
  Specifies that the system marks a pool member **up** or **down** based on the response of the server at the IP address and port supplied by the pool member.

- ***:<port>**
  Specifies that the system marks a pool member **up** or **down** based on the response of the server at the IP address supplied by the pool member and the port you specify.

- **<IP address>:<port>**
  Specifies that the system marks a pool member **up** or **down** based on the response of the server at the IP address and port you specify.

◆ filter
Specifications the SIP status codes that the target can return to be considered **up**. By default, the system always accepts status codes whose values are in the 100s, 200s, or 300s.

The options are:

- **any**
  Specifies that the monitor accepts any SIP status codes.

- **none**
  Specifies that the monitor does not accept any other SIP status codes. This is the default value.

- **status**
  Specifies one or more status codes that you want to add to the monitor.
◆ filter-neg
Specifies the SIP status codes that the target can return to be considered down. By default the system always accepts status codes according to sip-monitor.filter. After checking that, the status code is checked against this key. If a code is also in sip-monitor.filter, the node is marked up.

The options are:

- **any**
  Specifies that the monitor rejects all SIP status codes that are not in sip-monitor.filter.

- **none**
  Specifies that the monitor does not specifically reject any other SIP status codes. This is the default value.

- **status**
  Specifies one or more status codes that you want to add to the monitor.

◆ glob
Displays the items that match the glob expression. For a description of glob expression syntax, see the glob man page.

◆ headers
Specifies the set of SIP headers in the SIP message that is sent to the target. Separate each header with a new line. The default value is none.

◆ ignore-down-response
Specifies whether the monitor ignores a down response from the system it is monitoring. The default value is disabled.

◆ interval
Specifies the frequency at which the system issues the monitor check. The default value is 30 seconds.

◆ key
Specifies the key if the monitored target requires authentication. The default value is none.

◆ mode
Specifies the protocol that the monitor uses to communicate with the target.

The options are:

- **sips**
  Specifies that the monitor uses SIPS to communicate with the target.

- **tcp**
  Specifies that the monitor uses TCP to communicate with the target.

- **tls**
  Specifies that the monitor uses TLS to communicate with the target, and the SIP URI is SIPS.

- **udp**
  Specifies that the monitor uses UDP to communicate with the target.
◆ **name**
   Specifies a unique name for the component. This option is required for the commands `create`, `delete`, and `modify`.

◆ **partition**
   Displays the administrative partition in which the component resides.

◆ **probe-timeout**
   Specifies the number of seconds after which the BIG-IP system times out the probe request to the BIG-IP system. The default value is 5 seconds.

◆ **regex**
   Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. For a description of regular expression syntax, see the `regex` man page.

◆ **request**
   Specifies the SIP request line in the SIP message that is sent to the target. The default value is `none`.

◆ **timeout**
   Specifies the number of seconds the target has in which to respond to the monitor request. The default value is 120 seconds.

   If the target responds within the set time period, it is considered **up**. If the target does not respond within the set time period, it is considered **down**. Also, if the target responds with a RESET packet, the system immediately flags the target as **down** without waiting for the timeout interval to expire.

**See also**

`create`, `delete`, `edit`, `glob`, `gtm pool`, `list`, `modify`, `regex show`, `tmsh`
smtp

Configures a Simple Mail Transport Protocol (SMTP) monitor.

Module

gtm monitor

Syntax

Configure the smtp component within the gtm monitor module using the following syntax.

Create/Modify

create smtp [name]
modify smtp [name]

options:
  debug [no | yes]
  defaults-from [name]
  description [string]
  destination [ip address][port]
  domain [ [name] | none]
  ignore-down-response [enabled | disabled]
  interval [integer]
  probe-timeout [integer]
  timeout [integer]

edit smtp [ [name] | [glob] | [regex] ] ... 

options:
  all-properties
  non-default properties

Display

list smtp
list smtp [ [name] | [glob] | [regex] ] ... 
show running-config smtp
show running-config smtp [ [name] | [glob] | [regex] ] ... 

options:
  all-properties
  non-default-properties
  one-line
  partition
Delete

\texttt{delete smtp [name]}

\begin{itemize}
\item \textbf{Note}
\textit{You cannot delete default monitors.}
\end{itemize}

Description

You can use the \texttt{smtp} component to configure a custom monitor, or you can use the default SMTP monitor that the Global Traffic Manager provides. This type of monitor checks the status of a pool, pool member, or virtual server by issuing standard SMTP commands.

Examples

Creates a monitor named \texttt{my_smtp} that inherits properties from the default SMTP monitor:

\texttt{create smtp my_smtp defaults-from smtp}

Displays the properties of all of the SMTP monitors:

\texttt{list smtp}

Options

You can use these options with the \texttt{smtp} component:

\begin{itemize}
\item \textbf{debug}
  Specifies whether the monitor sends error messages and additional information to a log file created and labeled specifically for this monitor. You can use the log information to help diagnose and troubleshoot unsuccessful health checks. The default value is \texttt{no}.
  The options are:
  \begin{itemize}
  \item \texttt{no}
    Specifies that the system does not redirect error messages and additional information related to this monitor.
  \item \texttt{yes}
    Specifies that the system redirects error messages and additional information to the \texttt{/var/log/<monitor_type>_<ip address>_<port>.log} file.
  \end{itemize}
\item \textbf{defaults-from}
  Specifies the name of the monitor from which you want your custom monitor to inherit settings. The default value is \texttt{smtp}.
\item \textbf{description}
  User-defined description.
\end{itemize}
• **destination**
  Specifies the IP address and service port of the resource that is the destination of this monitor. The default value is *:*.

Possible values are:

- ***:**
  Specifies that the system marks a pool member **up** or **down** based on the response of the server at the IP address and port supplied by the pool member.

- ***:port**
  Specifies that the system marks a pool member **up** or **down** based on the response of the server at the IP address supplied by the pool member and the port you specify.

- **<IP address>:<port>**
  Specifies that the system marks a pool member **up** or **down** based on the response of the server at the IP address and port you specify.

• **domain**
  Specifies the domain name to check, for example: **bigipinternal.com**. The default value is **none**.

• **glob**
  Displays the items that match the **glob** expression. For a description of **glob** expression syntax, see the **glob** man page.

• **ignore-down-response**
  Specifies whether the monitor ignores a down response from the system it is monitoring. The default value is **disabled**.

• **interval**
  Specifies the frequency at which the system issues the monitor check. The default value is 30 seconds.

• **name**
  Specifies a unique name for the component. This option is required for the commands **create**, **delete**, and **modify**.

• **partition**
  Displays the administrative partition in which the component resides.

• **probe-timeout**
  Specifies the number of seconds after which the BIG-IP system times out the probe request to the BIG-IP system. The default value is 5 seconds.

• **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. For a description of regular expression syntax, see the **regex** man page.

• **timeout**
  Specifies the number of seconds the target has in which to respond to the monitor request. The default value is 120 seconds.
If the target responds within the set time period, it is considered **up**. If the target does not respond within the set time period, it is considered **down**.
Also, if the target responds with a RESET packet, the system immediately flags the target as **down** without waiting for the timeout interval to expire.

### See also

- create, delete, edit, glob, gtm pool, list, modify, regex show, tmsh
**gtm monitor Module Components**

### snmp

Configures a Simple Network Management Protocol (SNMP) monitor.

### Module

**gtm monitor**

### Syntax

Configure the `snmp` component within the `gtm monitor` module using the following syntax.

#### Create/Modify

- `create snmp [name]`
- `modify snmp [name]`

  **options:**
  - `community [ [name] | none]`
  - `defaults-from [name]`
  - `description [string]`
  - `destination [ip address] [port]`
  - `ignore-down-response [enabled | disabled]`
  - `interval [integer]`
  - `port [ [integer] | none]`
  - `probe attempts [integer]`
  - `probe-interval [integer]`
  - `probe-timeout [integer]`
  - `timeout [integer]`
  - `version [ [integer] | none]`

- `edit snmp [ [name] | [glob] | [regex] ] ... ]`

  **options:**
  - `all-properties`
  - `non-default properties`

#### Display

- `list snmp`  
- `list snmp [ [name] | [glob] | [regex] ] ... ]`
- `show running-config snmp`  
- `show running-config snmp [ [name] | [glob] | [regex] ] ... ]`

  **options:**
  - `all-properties`
  - `non-default-properties`
  - `one-line`
  - `partition`
Delete

\texttt{delete snmp \{name\}}

\textbf{Note}

\textit{You cannot delete default monitors.}

Description

You can use the \texttt{snmp} component to configure a custom monitor, or you can use the default SNMP monitor that the Global Traffic Manager provides. The SNMP monitor is both a health and performance monitor. This type of monitor checks the performance of a server running an SNMP agent such as UC Davis, for the purpose of load balancing traffic to that server.

Examples

Creates a monitor named \texttt{my\_snmp} that inherits properties from the default SNMP monitor:

\texttt{create snmp my\_snmp defaults-from snmp\_gtm}

Displays the properties of all of the SNMP monitors:

\texttt{list snmp}

Options

You can use these options with the \texttt{snmp} component:

\begin{itemize}
  \item \texttt{community}
    Specifies the community name that the BIG-IP system must use to authenticate with the host server through SNMP. The default value is \texttt{public}.
  \item \texttt{defaults-from}
    Specifies the name of the monitor from which you want your custom monitor to inherit settings. The default value is \texttt{snmp\_gtm}.
  \item \texttt{description}
    User-defined description.
  \item \texttt{destination}
    Specifies the IP address and service port of the resource that is the destination of this monitor. The default value is \texttt{*:*}.
    Possible values are:
    \begin{itemize}
      \item \texttt{*:*}
        Specifies that the system marks a pool member \texttt{up} or \texttt{down} based on the response of the server at the IP address and port supplied by the pool member.
    \end{itemize}
\end{itemize}
gtm monitor Module Components

- `*:port`
  Specifies that the system marks a pool member up or down based on the response of the server at the IP address supplied by the pool member and the port you specify.

- `<IP address>:<port>`
  Specifies that the system marks a pool member up or down based on the response of the server at the IP address and port you specify.

- `glob`
  Displays the items that match the glob expression. For a description of glob expression syntax, see the glob man page.

- `ignore-down-response`
  Specifies whether the monitor ignores a down response from the system it is monitoring. The default value is disabled.

- `interval`
  Specifies the frequency at which the system issues the monitor check. The default value is 90 seconds.

- `name`
  Specifies a unique name for the component. This option is required for the commands create, delete, and modify.

- `partition`
  Displays the administrative partition in which the component resides.

- `port`
  Specifies the port number to which this monitor sends SNMP traps. The default value is 161.

- `probe-attempts`
  Specifies the number of times the BIG-IP system attempts to probe the host server, after which the BIG-IP system considers the host server down or unavailable. The default value is 1.

- `probe-interval`
  Specifies the frequency at which the BIG-IP system probes the host server. The default value is 0.

- `probe-timeout`
  Specifies the number of seconds after which the BIG-IP system times out the probe request to the BIG-IP system. The default value is 5 seconds.

- `regex`
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. For a description of regular expression syntax, see the regex man page.

- `timeout`
  Specifies the number of seconds the target has in which to respond to the monitor request. The default value is 180 seconds.

  If the target responds within the set time period, it is considered up. If the target does not respond within the set time period, it is considered down. Also, if the target responds with a RESET packet, the system immediately flags the target as down without waiting for the timeout interval to expire.
◆ **version**  
Specifies the SNMP version the monitor uses. The default value is **none**.

**See also**

create, delete, edit, glob, gtm pool, list, modify, regex show, tmsh
snmp-link

Configures a Simple Network Management Protocol (SNMP) link monitor.

Module

gtm monitor

Syntax

Configure the snmp-link component within the gtm monitor module using the following syntax.

Create/Modify

create snmp-link [name]
modify snmp-link [name]

options:
  community [ [name] | none]
  defaults-from [name]
  description [string]
  destination [ip address]
  ignore-down-response [enabled | disabled]
  interval [integer]
  port [ [integer] | none]
  probe-attempts [integer]
  probe-interval [integer]
  probe-timeout [integer]
  timeout [integer]
  version [ [integer] | none]

edit snmp-link [ [name] | [glob] | [regex] ] ... }

options:
  all-properties
  non-default properties

Display

list snmp-link
list snmp-link [ [name] | [glob] | [regex] ] ... ]

show running-config snmp-link
show running-config snmp-link [ [name] | [glob] | [regex] ] ... ]

options:
  all-properties
  non-default-properties
  one-line
  partition
Delete

    delete snmp-link [name]

◆ Note

You cannot delete default monitors.

Description

You can use the snmp-link component to configure a custom monitor, or you can use the default SNMP Link monitor that the Global Traffic Manager provides. This type of monitor checks the current CPU, memory, and disk usage of a pool, pool member, or virtual server that is running an SNMP data collection agent, and then dynamically load balances traffic accordingly.

Examples

Creates a monitor named my_snmp-link that inherits properties from the default SNMP Link monitor:

    create snmp-link my_snmp-link defaults-from snmp_link

Displays the properties of all of the SNMP link monitors:

    list snmp-link

Options

You can use these options with the snmp-link component:

◆ community
   Specifies the community to which the SNMP Link monitor belongs. The default value is public.

◆ defaults-from
   Specifies the name of the monitor from which you want your custom monitor to inherit settings. The default value is snmp_link.

◆ description
   User-defined description.

◆ destination
   Specifies the IP address of the resource that is the destination of this monitor. The default value is *.

Possible values are:

◆ *
   Specifies that the system performs a health check on the IP address of the node.
• `<IP address>`
  Specifies that the system performs a health check on the IP address
  that you specify, routes the check through the IP address of the
  associated node, and marks the IP address of the associated node **up**
  or **down** accordingly.

  ◆ **glob**
  Displays the items that match the `glob` expression. For a description of
  `glob` expression syntax, see the `glob` man page.

  ◆ **ignore-down-response**
  Specifies whether the monitor ignores a down response from the system
  it is monitoring. The default value is **disabled**.

  ◆ **interval**
  Specifies the frequency at which the system issues the monitor check.
  The default value is **10** seconds.

  ◆ **name**
  Specifies a unique name for the component. This option is required for
  the commands **create**, **delete**, and **modify**.

  ◆ **partition**
  Displays the administrative partition in which the component resides.

  ◆ **port**
  Specifies the port number to which this monitor sends SNMP traps. The
  default value is **161**.

  ◆ **probe-attempts**
  Specifies the number of times the BIG-IP system attempts to probe the
  host server, after which the BIG-IP system considers the host server
  **down** or unavailable. The default value is **3**.

  ◆ **probe-interval**
  Specifies the frequency at which the BIG-IP system probes the host
  server. The default value is **0**.

  ◆ **probe-timeout**
  Specifies the number of seconds after which the BIG-IP system times out
  the probe request to the BIG-IP system. The default value is **5** seconds.

  ◆ **regex**
  Displays the items that match the regular expression. The regular
  expression must be preceded by an at sign (`@[regular expression]`) to
  indicate that the identifier is a regular expression. For a description of
  regular expression syntax, see the `regex` man page.

  ◆ **timeout**
  Specifies the number of seconds the target has in which to respond to the
  monitor request. The default value is **30** seconds.
  
  If the target responds within the set time period, it is considered **up**. If the
  target does not respond within the set time period, it is considered **down**. Also, if the target responds with a RESET packet, the system
  immediately flags the target as **down** without waiting for the timeout
  interval to expire.

  ◆ **version**
  Specifies the SNMP version the monitor uses. The default value is **none**.
See also

create, delete, edit, glob, list, ltm node, modify, regex, show, tmsh
soap

Configures a Simple Object Access Protocol (SOAP) monitor.

Module

gtm monitor

Syntax

Configure the soap component within the gtm monitor module using the following syntax.

Create/Modify

create soap [name]
modify soap [name]

options:
  debug [no | yes]
  defaults-from [name]
  description [string]
  destination [ip address][port]
  expect-fault [no | yes]
  ignore-down-response [enabled | disabled]
  interval [integer]
  method [string]
  namespace [ [name] | none]
  parameter-name [ [name] | none]
  parameter-type [bool | int | long | [string] ]
  parameter-value [none | [integer] | [string] ]
  password [none | [password] ]
  probe-timeout [integer]
  protocol [ [none] | [protocol] ]
  return-type [bool | char | double | int | long | short | [string] ]
  return-value [none | [integer] | [string] ]
  timeout [integer]
  url-path [none | [string] ]
  username [ [name] | none]

ead external [ [name] | [glob] | [regex] ] ... }

options:
  all-properties
  non-default properties
Display

```
list soap
list soap [ [name] | [glob] | [regex] ] ... ]
show running-config soap
show running-config soap [ [name] | [glob] | [regex] ] ... ]
options:
  all-properties
  non-default-properties
  one-line
  partition
```

Delete

```
delete soap [name]
```

◆ Note

You cannot delete default monitors.

Description

You can use the soap component to configure a custom monitor, or you can use the default SOAP monitor that the Global Traffic Manager provides. This type of monitor tests a web service based on SOAP.

Examples

Creates a monitor named my_soap that inherits properties from the default SOAP monitor:
```
create soap my_soap defaults-from soap
```

Displays the properties of all of the SOAP monitors:
```
list soap
```

Options

You can use these options with the soap component:

◆ debug
  Specifies whether the monitor sends error messages and additional information to a log file created and labeled specifically for this monitor. You can use the log information to help diagnose and troubleshoot unsuccessful health checks. The default value is no.

  The options are:
- **no**
  Specifies that the system does not redirect error messages and additional information related to this monitor.

- **yes**
  Specifies that the system redirects error messages and additional information to the 
  `/var/log/<monitor_type>_<ip address>.<port>.log` file.

- **defaults-from**
  Specifies the name of the monitor from which you want your custom monitor to inherit settings. The default value is `soap`.

- **description**
  User-defined description.

- **destination**
  Specifies the IP address and service port of the resource that is the destination of this monitor. The default value is `*::*`. Possible values are:
  - `*::*`
    Specifies that the system marks a pool member up or down based on the response of the server at the IP address and port supplied by the pool member.
  - `*:port`
    Specifies that the system marks a pool member up or down based on the response of the server at the IP address supplied by the pool member and the port you specify.
  - `<IP address>:<port>`
    Specifies that the system marks a pool member up or down based on the response of the server at the IP address and port you specify.

- **expect-fault**
  Specifies whether the value of the `method` option causes the monitor to expect a SOAP fault message. The default value is `no`.

- **glob**
  Displays the items that match the `glob` expression. For a description of `glob` expression syntax, see the `glob` man page.

- **ignore-down-response**
  Specifies whether the monitor ignores a down response from the system it is monitoring. The default value is `disabled`.

- **interval**
  Specifies the frequency at which the system issues the monitor check. The default value is 30 seconds.

- **method**
  Specifies the method by which the monitor contacts the resource.

- **name**
  Specifies a unique name for the component. This option is required for the commands `create`, `delete`, and `modify`. 
- **namespace**
  Specifies the name space for the web service you are monitoring, for example: `http://example.com/`. The default value is `none`.

- **parameter-name**
  If the method has a parameter, specifies the name of that parameter. The default value is `bool`.

- **parameter-type**
  Specifies the parameter type. The default value is `none`.

- **parameter-value**
  Specifies the value for the parameter. The default value is `none`.

- **partition**
  Displays the administrative partition in which the component resides.

- **password**
  Specifies the password if the monitored target requires authentication. The default value is `none`.

- **probe-timeout**
  Specifies the number of seconds after which the BIG-IP system times out the probe request to the BIG-IP system. The default value is 5 seconds.

- **protocol**
  Specifies the protocol that the monitor uses to communicate with the target. The default value is `none`.

- **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (`@[regular expression]`) to indicate that the identifier is a regular expression. For a description of regular expression syntax, see the `regex` man page.

- **return-type**
  Specifies the type for the returned parameter. The default value is `bool`.

- **return-value**
  Specifies the value for the returned parameter. The default value is `none`.

- **timeout**
  Specifies the number of seconds the target has in which to respond to the monitor request. The default value is 120 seconds.

  If the target responds within the set time period, it is considered **up**. If the target does not respond within the set time period, it is considered **down**. Also, if the target responds with a RESET packet, the system immediately flags the target as **down** without waiting for the timeout interval to expire.

- **url-path**
  Specifies the URL for the web service that you are monitoring, for example: `/services/myservice.aspx`. The default value is `none`.

- **username**
  Specifies the user name if the monitored target requires authentication. The default value is `none`. 
See also

create, delete, edit, glob, gtm pool, list, modify, regex show, tmsh
Configure a Transmission Control Protocol (TCP) monitor.

**Module**

*gtm monitor*

**Syntax**

Configure the `tcp` component within the *gtm monitor* module using the following syntax.

**Create/Modify**

```plaintext
create tcp [name]
modify tcp [name]
  options:
    defaults-from [name]
    description [string]
    destination [ip address][port]
    ignore-down-response [enabled | disabled]
    interval [integer]
    probe-timeout [integer]
    recv [none | [string] ]
    reverse [enabled | disabled]
    send [none | [string] ]
    timeout [integer]
    transparent [disabled | enabled]
```

```plaintext
edit tcp [ [name] | [glob] | [regex] ] ... ]
  options:
    all-properties
    non-default properties
```

**Display**

```plaintext
list tcp
list tcp [ [name] | [glob] | [regex] ] ... ]

show running-config tcp
show running-config tcp [ [name] | [glob] | [regex] ] ... ]
  options:
    all-properties
    non-default-properties
    one-line
    partition
```
Delete

\texttt{delete tcp [name]}

\textbf{Note}

\textit{You cannot delete default monitors.}

Description

You can use the \texttt{tcp} component to configure a custom monitor, or you can use the default TCP monitor that the Global Traffic Manager provides.

Examples

Creates a monitor named \texttt{my\_tcp} that inherits properties from the default TCP monitor:

\texttt{create tcp my\_tcp defaults-from tcp}

Displays the properties of all of the TCP monitors:

\texttt{list tcp}

Options

You can use these options with the \texttt{tcp} component:

\begin{itemize}
  \item \texttt{defaults-from}
    Specifies the name of the monitor from which you want your custom monitor to inherit settings. The default value is \texttt{tcp}.
  \item \texttt{description}
    User-defined description.
  \item \texttt{destination}
    Specifies the IP address and service port of the resource that is the destination of this monitor. The default value is \texttt{*:}.
    \begin{itemize}
      \item \texttt{*:}
        Specifies that the system marks a pool member up or down based on the response of the server at the IP address and port supplied by the pool member.
      \item \texttt{*:port}
        Specifies that the system marks a pool member up or down based on the response of the server at the IP address supplied by the pool member and the port you specify.
      \item \texttt{<IP address>:<port>}
        Specifies that the system marks a pool member up or down based on the response of the server at the IP address and port you specify.
    \end{itemize}
\end{itemize}
Chapter 21

- `<IP address>:<port>` (with the `transparent` option enabled)
  Specifies that the system performs a health check on the server at the IP address and port you specify, routes the check through the IP address and port supplied by the pool member, and marks the pool member (the gateway) up or down accordingly.

- `glob`
  Displays the items that match the `glob` expression. For a description of `glob` expression syntax, see the `glob` man page.

- `ignore-down-response`
  Specifies whether the monitor ignores a down response from the system it is monitoring. The default value is `disabled`.

- `interval`
  Specifies the frequency at which the system issues the monitor check. The default value is 30 seconds.

- `name`
  Specifies a unique name for the component. This option is required for the commands `create`, `delete`, and `modify`.

- `partition`
  Displays the administrative partition in which the component resides.

- `probe-timeout`
  Specifies the number of seconds after which the BIG-IP system times out the probe request to the BIG-IP system. The default value is 5 seconds.

- `recv`
  Specifies the text string that the monitor looks for in the returned resource. The default value is `none`.
  The most common receive expressions contain a text string that is included in an HTML file on your site. The text string can be regular text, HTML tags, or image names. If you do not specify a value for both the `send` and `recv` options, the monitor performs a simple service check and connect only.

- `regex`
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. For a description of regular expression syntax, see the `regex` man page.

- `reverse`
  Specifies whether the monitor operates in reverse mode. When the monitor is in reverse mode, a successful check marks the monitored object down instead of up. You can use this mode only if you configure both the `send` and `recv` options.
  The default value is `disabled`, which specifies that the monitor does not operate in reverse mode. The `enabled` value specifies that the monitor operates in reverse mode.

- `send`
  Specifies the text string that the monitor sends to the target object. The default value is `GET /`, which retrieves a default HTML file for a web site.
To retrieve a specific page from a web site, specify a fully-qualified path name, for example: `GET /www/company/index.html`. Since the string can have special characters, the system can require that the string be enclosed with single quotation marks.

If this value is null, then a valid connection suffices to determine that the service is **up**. In this case, the system does not need the `recv` option and ignores the option even if not null.

- **timeout**
  Specifies the number of seconds the target has in which to respond to the monitor request. The default value is **120** seconds.

  If the target responds within the set time period, it is considered **up**. If the target does not respond within the set time period, it is considered **down**. Also, if the target responds with a RESET packet, the system immediately flags the target as **down** without waiting for the timeout interval to expire.

- **transparent**
  Specifies whether the monitor operates in transparent mode. Monitors in transparent mode can monitor pool members through firewalls. The default value is **disabled**.

**See also**

create, delete, edit, glob, gtm pool, gtm server, list, modify, regex, show, tmsh
tcp-half-open

Configures a Transmission Control Protocol (TCP) Half Open monitor.

Module

gtm monitor

Syntax

Configure the tcp-half-open component within the gtm monitor module using the following syntax.

Create/Modify

create tcp-half-open [name]
modify tcp-half-open [name]
   options:
      defaults-from [name]
      description [string]
      destination [ip address][port]
      ignore-down-response [enabled | disabled]
      interval [integer]
      probe-attempts [integer])
      probe-interval [integer])
      probe-timeout [integer]
      timeout [integer]
      transparent [disabled | enabled]
edit tcp-half-open [ [name] | [glob] | [regex] ] ... ]
   options:
      all-properties
      non-default properties

Display

list tcp-half-open
list tcp-half-open [ [name] | [glob] | [regex] ] ... ]
show running-config tcp-half-open
show running-config tcp-half-open [ [name] | [glob] | [regex] ] ... ]
   options:
      all-properties
      non-default-properties
      one-line
      partition
Delete

delete tcp-half-open [name]

◆ Note

You cannot delete default monitors.

Description

You can use the tcp-half-open component to configure a custom monitor, or you can use the default TCP Half Open monitor that the Global Traffic Manager provides.

Examples

Creates a monitor named my_tcp-half-open that inherits properties from the default TCP Half Open monitor:

create tcp-half-open my_tcp-half-open defaults-from tcp_half_open

Displays the properties of all of the TCP Half Open monitors:

list tcp-half-open

Options

You can use these options with the tcp-half-open component:

◆ defaults-from
   Specifies the name of the monitor from which you want your custom monitor to inherit settings. The default value is tcp_half_open.

◆ description
   User-defined description.

◆ destination
   Specifies the IP address and service port of the resource that is the destination of this monitor. The default value is *:*.
   Possible values are:
   • *:*  
     Specifies that the system marks a pool member up or down based on the response of the server at the IP address and port supplied by the pool member.
   • *:port
     Specifies that the system marks a pool member up or down based on the response of the server at the IP address supplied by the pool member and the port you specify.
   • <IP address>:<port>
     Specifies that the system marks a pool member up or down based on the response of the server at the IP address and port you specify.
- `<IP address>:<port>` (with the `transparent` option enabled)
  Specifies that the system performs a health check on the server at the IP address and port you specify, routes the check through the IP address and port supplied by the pool member, and marks the pool member (the gateway) up or down accordingly.

- `glob`
  Displays the items that match the `glob` expression. For a description of `glob` expression syntax, see the `glob` man page.

- `ignore-down-response`
  Specifies whether the monitor ignores a down response from the system it is monitoring. The default value is `disabled`.

- `interval`
  Specifies the frequency at which the system issues the monitor check. The default value is 30 seconds.

- `name`
  Specifies a unique name for the component. This option is required for the commands `create`, `delete`, and `modify`.

- `partition`
  Displays the administrative partition in which the component resides.

- `probe-attempts`
  Specifies the number of times the BIG-IP system attempts to probe the host server, after which the BIG-IP system considers the host server down or unavailable. The default value is 3.

- `probe-interval`
  Specifies the frequency at which the BIG-IP system probes the host server. The default value is 1.

- `probe-timeout`
  Specifies the number of seconds after which the BIG-IP system times out the probe request to the BIG-IP system. The default value is 5 seconds.

- `regex`
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. For a description of regular expression syntax, see the `regex` man page.

- `timeout`
  Specifies the number of seconds the target has in which to respond to the monitor request. The default value is 120 seconds.

  If the target responds within the set time period, it is considered up. If the target does not respond within the set time period, it is considered down. Also, if the target responds with a RESET packet, the system immediately flags the target as down without waiting for the timeout interval to expire.

- `transparent`
  Specifies whether the monitor operates in transparent mode. Monitors in transparent mode can monitor pool members through firewalls. The default value is `disabled`. 

See also

create, delete, edit, glob, gtm pool, gtm server, list, modify, regex, show, tmsh
udp

Configures a User Datagram Protocol (UDP) monitor.

Module

gtm monitor

Syntax

Configure the udp component within the gtm monitor module using the following syntax.

Create/Modify

create udp [name]
modify udp [name]
  options:
    debug [no | yes]
    defaults-from [name]
    description [string]
    destination [ip address][port]
    ignore-down-response [enabled | disabled]
    interval [integer]
    probe-attempts [integer]
    probe-interval [integer]
    probe-timeout [integer]
    send [none | [string]]
    send-packets [integer]
    timeout [integer]
    timeout-packets [ [integer] | none]
    transparent [disabled | enabled]
edit udp [ [name] | [glob] | [regex] ] ...]
  options:
    all-properties
    non-default properties

Display

list udp
list udp [ [name] | [glob] | [regex] ] ...]
show running-config udp
show running-config udp [ [name] | [glob] | [regex] ] ...]
  options:
**Delete**

```
delete udp [name]
```

**Note**

*You cannot delete default monitors.*

**Description**

You can use the `udp` component to configure a custom monitor, or you can use the default UDP monitor that the Global Traffic Manager provides. This type of monitor verifies the UDP service by attempting to send UDP packets to a pool, pool member, or virtual server, and then receiving a reply.

**Examples**

Creates a monitor named `my_udp` that inherits properties from the default UDP monitor:

```
create udp my_udp defaults-from udp
```

Displays the properties of all of the UDP monitors:

```
list udp
```

**Options**

You can use these options with the `udp` component:

- **debug**
  
  Specifies whether the monitor sends error messages and additional information to a log file created and labeled specifically for this monitor. You can use the log information to help diagnose and troubleshoot unsuccessful health checks. The default value is `no`.

  The options are:
  
  - **no**
    
    Specifies that the system does not redirect error messages and additional information related to this monitor.
  
  - **yes**
    
    Specifies that the system redirects error messages and additional information to the `[/var/log/<monitor_type>_<ip address>_<port>.log]` file.
- **defaults-from**
  Specifies the name of the monitor from which you want your custom monitor to inherit settings. The default value is `udp`.

- **description**
  User-defined description.

- **destination**
  Specifies the IP address and service port of the resource that is the destination of this monitor. The default value is `*:*

  Possible values are:
  - `*:*
    Specifies that the system marks a pool member **up** or **down** based on the response of the server at the IP address and port supplied by the pool member.
  - `*:port`
    Specifies that the system marks a pool member **up** or **down** based on the response of the server at the IP address supplied by the pool member and the port you specify.
  - `<IP address>:<port>`
    Specifies that the system marks a pool member **up** or **down** based on the response of the server at the IP address and port you specify.
  - `<IP address>:<port>` (with the **transparent** option **enabled**)
    Specifies that the system performs a health check on the server at the IP address and port you specify, routes the check through the IP address and port supplied by the pool member, and marks the pool member (the gateway) **up** or **down** accordingly.

- **glob**
  Displays the items that match the **glob** expression. For a description of **glob** expression syntax, see the **glob** man page.

- **ignore-down-response**
  Specifies whether the monitor ignores a down response from the system it is monitoring. The default value is **disabled**.

- **interval**
  Specifies the frequency at which the system issues the monitor check. The default value is 30 seconds.

- **name**
  Specifies a unique name for the component. This option is required for the commands **create**, **delete**, and **modify**.

- **partition**
  Displays the administrative partition in which the component resides.

- **probe-attempts**
  Specifies the number of times the BIG-IP system attempts to probe the host server, after which the BIG-IP system considers the host server **down** or unavailable. The default value is 3.

- **probe-interval**
  Specifies the frequency at which the BIG-IP system probes the host server. The default value is 1.
◆ **probe-timeout**
   Specifies the number of seconds after which the BIG-IP system times out the probe request to the BIG-IP system. The default value is 5 seconds.

◆ **regex**
   Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. For a description of regular expression syntax, see the `regex` man page.

◆ **send**
   Specifies the text string that the monitor sends to the target object. The default value is `send string`.

   To retrieve a specific page from a web site, specify a fully-qualified path name, for example: `GET /www/company/index.html`. Since the string can have special characters, the system can require that the string be enclosed with single quotation marks.

   If this value is null, then a valid connection suffices to determine that the service is up. In this case, the system does not need the value of the `recv` option and ignores the option even if not null.

◆ **send-packets**
   Specifies how many UDP packets that the monitor sends to the target. The default value is 2.

◆ **timeout**
   Specifies the number of seconds the target has in which to respond to the monitor request. The default value is 120 seconds.

   If the target responds within the set time period, it is considered up. If the target does not respond within the set time period, it is considered down. Also, if the target responds with a RESET packet, the system immediately flags the target as down without waiting for the timeout interval to expire.

◆ **timeout-packets**
   Specifies the number of seconds that the monitor waits for a response from the target. The default value is 2 seconds. If the monitor receives an ICMP error message response (node unreachable), the system considers the node down. If the monitor receives another response or no response, the system considers the node up.

◆ **transparent**
   Specifies whether the monitor operates in transparent mode. Monitors in transparent mode can monitor pool members through firewalls. The default value is disabled.

**See also**

create, delete, edit, glob, gtm pool, gtm server, list, modify, regex, show, tmsh
wap

Configures a Wireless Application Protocol (WAP) monitor.

Module

gtm monitor

Syntax

Configure the wap component within the gtm monitor module using the following syntax.

Create/Modify

create wap [name]
modify wap [name]

options:
  accounting-node [none | [RADIUS server name] ]
  accounting-port [ [integer] | none]
  call-id [none | [RADIUS server 11 digit phone number] ]
  check-until-up [enabled | disabled]
  debug [no | yes]
  defaults-from [name]
  description [string]
  destination [ip address][port]
  framed-address [none | [RADIUS framed IP address] ]
  ignore-down-response [enabled | disabled]
  interval [integer]
  probe-timeout [integer]
  recv [none | [string] ]
  secret [none | [password] ]
  send [none | [string] ]
  server-id [none | [RADIUS NAS-ID] ]
  session-id [none | [RADIUS session ID] ]
  timeout [integer]

edit wap [ [name] | [glob] | [regex] ] ... ]

options:
  all-properties
  non-default properties
Display

list wap
list wap [ [name] | [glob] | [regex] ] ... ]
show running-config wap
show running-config wap [ [name] | [glob] | [regex] ] ... ]
  options:
    all-properties
    non-default-properties
    one-line
    partition

Delete

delete wap [name]

◆ Note

You cannot delete default monitors.

Description

You can use the wap component to configure a custom monitor, or you can use the default WAP monitor that the Global Traffic Manager provides. This type of monitor requests the URL specified in the send option and finds the string specified in the recv option somewhere in the data returned by the URL response.

Examples

Creates a monitor named my_wap that inherits properties from the default WAP monitor:

create wap my_wap defaults-from wap

Displays the properties of all of the WAP monitors:

list wap

Options

You can use these options with the wap component:

◆ accounting-node
  Specifies the RADIUS server that provides authentication for the WAP target. If you configure the accounting-port option, but you do not configure the this option, the system assumes that the RADIUS server and the WAP server are the same system.
◆ **accounting-port**
Specifies the port that the monitor uses for RADIUS accounting. The default value is **none**. A value of **0** (zero) disables RADIUS accounting.

◆ **call-id**
Specifies the 11-digit phone number for the RADIUS server. The default value is **none**.

◆ **debug**
Specifies whether the monitor sends error messages and additional information to a log file created and labeled specifically for this monitor. You can use the log information to help diagnose and troubleshoot unsuccessful health checks. The default value is **no**.

The options are:
- **no**
  Specifies that the system does not redirect error messages and additional information related to this monitor.

- **yes**
  Specifies that the system redirects error messages and additional information to the 
  `/var/log/<monitor_type>_ip address_<port>.log` file.

◆ **defaults-from**
Specifies the name of the monitor from which you want your custom monitor to inherit settings. The default value is **wap**.

◆ **description**
User-defined description.

◆ **destination**
Specifies the IP address and service port of the resource that is the destination of this monitor. The default value is ***:***.

Possible values are:
- ***:***
  Specifies that the system marks a pool member **up** or **down** based on the response of the server at the IP address and port supplied by the pool member.

- **<IP address>:<port>**
  Specifies that the system marks a pool member **up** or **down** based on the response of the server at the IP address supplied by the pool member and the port you specify.

- **<IP address>:<port>**
  Specifies that the system marks a pool member **up** or **down** based on the response of the server at the IP address and port you specify.

◆ **framed-address**
Specifies the RADIUS framed IP address. The default value is **none**.

◆ **glob**
Displays the items that match the **glob** expression. For a description of **glob** expression syntax, see the **glob** man page.
- **ignore-down-response**  
  Specifies whether the monitor ignores a down response from the system it is monitoring. The default value is `disabled`.

- **interval**  
  Specifies the frequency at which the system issues the monitor check. The default value is 10 seconds.

- **name**  
  Specifies a unique name for the component. This option is required for the commands `create`, `delete`, and `modify`.

- **partition**  
  Displays the administrative partition in which the component resides.

- **probe-timeout**  
  Specifies the number of seconds after which the BIG-IP system times out the probe request to the BIG-IP system. The default value is 5 seconds.

- **recv**  
  Specifies the text string that the monitor looks for in the returned resource. The most common receive expressions contain a text string that is included in an HTML file on your site. The text string can be regular text, HTML tags, or image names. If you do not specify both a value for both the `send` and `recv` options, the monitor performs a simple service check and connect only. The default value is `none`.

- **regex**  
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. For a description of regular expression syntax, see the `regex` man page.

- **secret**  
  Specifies the password the monitor needs to communicate with the resource. The default value is `none`.

- **send**  
  Specifies the text string that the monitor sends to the target object. The default value is `GET /`, which retrieves a default HTML file for a web site.

  To retrieve a specific page from a web site, specify a fully-qualified path name, for example: `GET/www/company/index.html`. Since the string can have special characters, the system can require that the string be enclosed with single quotation marks.

  If this value is null, then a valid connection suffices to determine that the service is up. In this case, the system does not need the `recv` option and ignores the option even if it is not null. The default value is `none`.

- **server-id**  
  Specifies the RADIUS NAS-ID for this system when configuring a RADIUS server. The default value is `none`.

- **session-id**  
  Specifies the RADIUS session identification number when configuring a RADIUS server. The default value is `none`.
timeout
Specifies the number of seconds the target has in which to respond to the monitor request. The default value is 31 seconds.
If the target responds within the set time period, it is considered up. If the target does not respond within the set time period, it is considered down. Also, if the target responds with a RESET packet, the system immediately flags the target as down without waiting for the timeout interval to expire.

See also
create, delete, edit, glob, gtm pool, list, modify, regex show, tmsh
**wmi**

Configures a Windows Management Instrumentation (WMI) monitor.

**Module**

`gtm monitor`

**Syntax**

Configure the `wmi` component within the `gtm monitor` module using the following syntax.

**Create/Modify**

```plaintext
create wmi [name]
modify wmi [name]
```

**options:**

```plaintext
command [ [command] | none]
defaults-from [name]
description [string]
ignore-down-response [enabled | disabled]
interval [integer]
metrics [ [value] | none]
password [none | [password] ]
probe-timeout [integer]
timeout [integer]
url [none | [URL] ]
username [ [name] | none]
```

```plaintext
edit wmi [ [name] | [glob] | [regex] ] ... ]
```

**options:**

```plaintext
all-properties
non-default properties
```

**Display**

```plaintext
list wmi
list wmi [ [name] | [glob] | [regex] ] ... ]
show running-config wmi
show running-config wmi [ [name] | [glob] | [regex] ] ... ]
```

**options:**

```plaintext
agent
all-properties
method
```
Delete

delete wmi [name]

◆ Note

You cannot delete default monitors.

Description

You can use the wmi component to configure a custom monitor, or you can use the default WMI monitor that the Global Traffic Manager provides. This type of monitor checks the performance of a pool, pool member, or virtual server that is running the WMI data collection agent, and then dynamically load balances traffic accordingly.

Examples

Creates a monitor named my_wmi that inherits properties from the default WMI monitor:

create wmi my_wmi defaults-from wmi

Displays the properties of all of the WMI monitors:

list wmi

Options

You can use these options with the wmi component:

◆ agent
   Displays the agent for the monitor. The default agent is Mozilla/4.0 (compatible: MSIE 5.0; Windows NT). You cannot modify the agent.

◆ command
   Specifies the command that the system uses to obtain the metrics from the resource. See the documentation for this resource for information on available commands.

◆ defaults-from
   Specifies the name of the monitor from which you want your custom monitor to inherit settings. The default value is wmi.

◆ description
   User-defined description.
- **glob**
  Displays the items that match the `glob` expression. For a description of `glob` expression syntax, see the `glob` man page.

- **ignore-down-response**
  Specifies whether the monitor ignores a down response from the system it is monitoring. The default value is **disabled**.

- **interval**
  Specifies the frequency at which the system issues the monitor check. The default value is **30 seconds**.

- **method**
  Displays the GET method. You cannot modify the method.

- **metrics**
  Specifies the performance metrics that the commands collect from the target. The default value is **LoadPercentage, DiskUsage, PhysicalMemoryUsage:1.5, VirtualMemoryUsage:2.0**.

- **name**
  Specifies a unique name for the component. This option is required for the commands **create**, **delete**, and **modify**.

- **partition**
  Displays the administrative partition in which the component resides.

- **password**
  Specifies the password if the monitored target requires authentication. The default value is **none**.

- **post**
  Specifies the mechanism that the monitor uses for posting. The default value is **RespFormat=HTML**. You cannot change the post format for WMI monitors.

- **probe-timeout**
  Specifies the number of seconds after which the BIG-IP system times out the probe request to the BIG-IP system. The default value is **5 seconds**.

- **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. For a description of regular expression syntax, see the `regex` man page.

- **timeout**
  Specifies the number of seconds the target has in which to respond to the monitor request. The default value is **120 seconds**.

  If the target responds within the set time period, it is considered **up**. If the target does not respond within the set time period, it is considered **down**. Also, if the target responds with a RESET packet, the system immediately flags the target as **down** without waiting for the timeout interval to expire.

- **url**
  Specifies the URL that the monitor uses. The default value is **/scripts/f5Isapi.dll**.
◆ username
   Specifies the user name if the monitored target requires authentication.
   The default value is none.

See also

create, delete, edit, glob, gtm pool, list, modify, regex show, tmsh
Ltm Module Components

- Introducing the Ltm module
- Alphabetical list of components
Introducing the ltm module

You can use the `tmsh` components that reside within the `ltm` module to configure Local Traffic Manager™. For more information about the `tmsh` hierarchical structure, see Chapter 2, *Understanding and Using the Traffic Management Shell*.

Alphabetical list of components

The remainder of this chapter lists the `tmsh` components that are available in the `ltm` module.
default-node-monitor

Configures the default node monitor for Local Traffic Manager™.

Module

ltm

Syntax

Configure the default-node-monitor component within the ltm module using the following syntax.

Create/Modify

modify default-node-monitor
  options:
    rule [rule syntax]
edit default-node-monitor
  options:
    all-properties

Display

list default-node-monitor
show running-config default-node-monitor
  options:
    one-line
    all-properties

Description

You can use the default-node-monitor component to modify the default pre-configured monitor that the system applies to any node address to which a monitor is not explicitly assigned.

Examples

Modifies the global default node monitor to use the rule ICMP:
modify default-node-monitor rule icmp

Displays the properties of the global default node monitor:
list default-node-monitor
Options

You can use this option to configure the `default-node-monitor` component:

- **rule**
  Specifies the rule that the system applies to any node that has not been assigned a monitor rule. The default value is none.
  
  You can specify:
  
  - A single monitor, for example:
    `modify default-node-monitor rule icmp`
  
  - Multiple monitors, for example:
    `modify default-node-monitor rule icmp and tcp_echo`
  
  - A minimum number of monitors, for example:
    `modify default-node-monitor rule min 1 of { icmp and tcp_echo }`

See also

`list`, `ltm node`, `modify`, `tmsh`
ifile

Configures the ifile component for Local Traffic Manager™.

Module

ltm

Syntax

Configure the ifile component within the ltm module using the syntax shown in the following sections.

Create/Modify

create ifile [name]
modify ifile [name]
options:
   description [string]
   file-name [ifile file object name]
edit ifile [ [name] | [glob] | [regex] ] ... 
options:
   all-properties
   non-default-properties
   one-line

Display

list ifile
list ifile [ [ [name] | [glob] | [regex] ] ... ]
show running-config ifile
show running-config ifile [ [ [name] | [glob] | [regex] ] ... ]
options:
   all-properties
   non-default-properties
   one-line

Description

You can use the ifile component to configure an iFile. The iFile can then be referenced from an iRule, to allow loading an external file into an iRule.
Examples

Creates an iFile named **my_ifile**, that gets its contents from the file object `ifile_file_object_name`.

```bash
create ifile my_ifile file-name ifile_file_object_name
```

Displays all of the properties of all of the iFiles.

```bash
list ifile all-properties
```

Deletes the iFile named **my_ifile**.

```bash
delete ifile my_ifile
```

Options

You can use these options with the **ifile** component:

- **description**
  User defined description.

- **file-name**
  The name of the iFile file object that this iFile uses.

See also

create, delete, edit, glob, list, modify, regex, tmsh
nat

Configures a network address translation (NAT) for Local Traffic Manager.

Module

ltm

Syntax

Configure the nat component within the ltm module using the following syntax.

Create/Modify

create nat [name]
modify nat [name]
options:
  arp
  auto-lasthop [default | enabled | disabled ]
  description [string]
  [enabled | disabled]
  originating-address [ip address]
  translation-address [ip address]
  traffic-group [string]
  vlans [enabled | disabled]
  vlans-disabled
  vlans-enabled
reset-stats nat
reset-stats nat [ [ [name] | [glob] | [regex] ] ... ]
edit nat [ [ [name] | [glob] | [regex] ] ... ]
options:
  all-properties
  non-default-properties

Display

list nat
list nat [ [ [name] | [glob] | [regex] ] ... ]
show running-config nat
show running-config nat [ [ [name] | [glob] | [regex] ] ... ]
options:
  all-properties
  non-default-properties
show nat
show nat [ [name] | [glob] | [regex] ] ... ]

options:
  (default | exa | gig | kil | meg | peta | raw | tera | yotta | zetta)
  field-fmt

Delete

   delete nat [name]

Description

A network address translation (NAT) defines a mapping between an originating IP address and an IP address that you specify.

A primary reason for defining a NAT is to allow one of the servers in the server array behind the traffic management system to start communication with a computer in front of, or external to, the system.

Examples

The node behind the system with the IP address 10.0.140.100 has a presence in front of the BIG-IP® system as IP address 11.0.0.100:

create nat new_nat translation-address 10.0.140.100
originating-address 11.0.0.100

Permanently deletes the NAT from the system configuration:

delete nat new_nat

Additional Restrictions

The nat component has the following additional restrictions:

- A virtual server cannot use the IP address specified in the NAT.
- A NAT should not use an IP address of a BIG-IP system.
- A NAT cannot use an originating or translated IP address defined for and used by a SNAT or another NAT.
- You must delete a NAT before you can redefine it.

Options

You can use these options with the nat component:

- **arp**
  Enables or disables Address Resolution Protocol (ARP). The default value is enabled.
- **description**
  User-defined description.

- **[enabled | disabled]**
  Enables or disables the NAT. The default value is **enabled**.

- **glob**
  Displays the items that match the **glob** expression. For a description of **glob** expression syntax, see the **glob** man page.

- **inherited-traffic-group**
  Indicates whether the **traffic-group** is inherited from the parent folder. This property is read only.

- **originating-address**
  Specifies the IP address from which traffic is being initiated.

- **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. For a description of regular expression syntax, see the **regex** man page.

- **traffic-group**
  Specifies the traffic group of the failover device group on which the NAT is active. The default traffic group is inherited from the containing folder.

- **translation-address**
  Specifies the IP address that is translated or mapped, and the IP address to which it is translated or mapped. This option is required when creating a NAT. This option cannot be changed after the **nat** has been created.

- **unit**
  Specifies the unit in a redundant system configuration. Derived from **traffic-group**. This property is read only.

- **vlans**
  Specifies a list of existing VLANs on which access to the NAT is enabled or disabled. A NAT is accessible on all VLANs by default.

- **vlans-disabled**
  Indicates the NAT is disabled on the list of VLANs.

- **vlans-enabled**
  Indicates the NAT is enabled on the list of VLANs.

**See also**

create, delete, edit, glob, list, ltm snat, ltm snat-translation, modify, regex, reset-stats, show, tmsh
ltm Module Components

node

Configures node addresses and services.

Module

ltm

Syntax

Configure the node component within the ltm module using the syntax in the following sections.

Create/Modify

create node [name]
modify node [name]
options:
  address [ip address]
  connection-limit [integer]
  description [string]
  [down | up]
  dynamic-ratio [integer]
  monitor [ [name] | none]
  rate-limit [integer]
  ratio [integer]
  session [user-enabled | user-disabled]
  state [user-down | user-up]
  metadata
    [add | delete | modify] {
      [metadata_name ...] {
        value [ "value content"
        persist [ true | false]
      }
    }
reset-stats node
  reset-stats node [ [ip address] | [glob] | [regex] ] ...
edit node [ [name] | [glob] | [regex] ] ...
options:
  all-properties
  non-default-properties

Display

list node
  list node [ [name] | [glob] | [regex] ] ...
show running-config node
  show running-config node [ [name] | [glob] | [regex] ] ...
options:
  all-properties
  non-default-properties
  one-line
  partition
  show node
show node [name]
  options:
    all-properties
    (default | exa | gig | kil | meg | peta | raw | tera | yotta | zetta)
    field-fmt

Delete
  delete node [name]

Description
Displays information about nodes, and sets attributes of nodes and node IP addresses.

Examples
  list node all-properties
  Displays all of the properties of all of the nodes.
  modify node all monitor none
  Removes all monitor associations from nodes.
  create node myNode address 10.10.10.15
  Creates a node named myNode with an IP address of 10.10.10.15.
  modify node myNode monitor none
  Removes all monitor associations from the node, myNode.
  show node
  Displays statistics and status for all nodes in the system configuration.
  show node all-properties
  Displays statistics and status for all nodes in the system configuration. If the system includes Packet Velocity® ASIC (PVA) and PVA Assist capabilities, this command displays status and statistics for that feature.

Options
  ◆ address
    Specifies the IP address of the node.
  ◆ connection-limit
    Specifies the maximum number of connections that a node or node address can handle. The default value is 0 (zero).
  ◆ description
    Specifies a user-defined description.
  ◆ [down | up]
    Marks the node up or down. The default value is down.
- **dynamic ratio**
  Sets the dynamic ratio number for the node. The ratio weights are based on continuous monitoring of the servers and are therefore continually changing. The default value is 1.
  Dynamic Ratio load balancing can currently be implemented on RealNetworks RealServer platforms, on Windows platforms equipped with Windows Management Instrumentation (WMI), or on a server equipped with either the UC Davis SNMP agent or Windows 2000 Server SNMP agent.

- **glob**
  Displays the items that match the glob expression. See `help glob` for a description of glob expression syntax.

- **metadata**
  Associates user defined data, each of which has a name and value pair and persistence. The default value is `persistent`, which saves the data to the config file.

- **monitor**
  Specifies the name of the monitor that you want to associate with the node. The default value is `none`.

- **partition**
  Displays the administrative partition in which the node object resides.

- **rate-limit**
  Specifies the maximum number of connections per second allowed for a node or node address. The default value is ‘disabled’.

- **ratio**
  Specifies the fixed ratio value used for a node during Ratio load balancing. The default value is 1.

- **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. See `help regex` for a description of regular expression syntax.

- **session**
  Establishing a session with a node is establishing the ability of the client to persist to the node when making new connections. When a node is session disabled, clients that have already established sessions with the node may create new connections, but a client that has not already established a session may not create a new one (or make a connection which would create a new session). This feature is used to gently drain connections from a node, typically as part of a maintenance operation. The default value is is `user-enabled`.

- **state**
  Specifies the current state of the node. Use `user-down` to indicate that the node may not handle any new connections. Use `user-up`, after using `user-down`, to indicate that the node may accept new connections.
See Also

create, delete, edit, glob, list, ltm pool, modify, regex, reset-stats, show, tmsh
pool

Configures load balancing pools for the Local Traffic Manager.

Module

ltm

Syntax

Modify the pool component within the ltm module using the syntax shown in the following sections.

Create/Modify

create pool [name]
modify pool [name]

options:
  all
  allow-nat [yes | no]
  allow-snat [yes | no]
  description [string]
  gateway-failsafe-device [string]
  ignore-persisted-weight [yes | no]
  ip-tos-to-client [pass-through | [integer] ]
  ip-tos-to-server [pass-through | [integer] ]
  link-qos-to-client [pass-through | [integer] ]
  link-qos-to-server [pass-through | [integer] ]
  load-balancing-mode [dynamic-ratio-member | dynamic-ratio-node | fastest-app-response | fastest-node | least-connections-members | least-connections-node | least-sessions | observed-member | observed-node | predictive-member | predictive-node | ratio-least-connections-member | ratio-least-connections-node | ratio-member | ratio-node | ratio-session | round-robin | weighted-least-connections-member | weighted-least-connections-node]
  members [add | delete | modify | replace-all-with] {
    [ [node_name:port] ] {
      options:
        address [ip address]
        connection-limit [integer]
        description [string]
        dynamic-ratio [integer]
        inherit-profile [enabled | disabled]
        monitor [name]
        priority-group [integer]
        profiles [none | profile_name]
        rate-limit [integer]
        ratio [integer]
        session [user-enabled | user-disabled]
        state [ user-up | user-down ]
      }
    }
  }

members none
metadata
  [add | delete | modify] {
    [metadata_name ...] {
      value ["value content"]
persist [true | false]
    }
  }
min-active-members [integer]
min-up-members [integer]
min-up-members-action [failover | reboot | restart-all]
min-up-members-checking [enabled | disabled]
monitor [name]
profiles [none | profile_name]
queue-on-connection-limit [enabled | disabled]
queue-depth-limit [integer]
queue-time-limit [integer]
reselect-tries [integer]
service-down-action [drop | none | reselect | reset]
slow-ramp-time [integer]
edit pool [ [ [name] | [glob] | [regex] ] ... ]
  options:
    all-properties
    non-default-properties
reset-stats pool
  reset-stats pool [ [ [name] | [glob] | [regex] ] ... ]

Display
list pool
  list pool [ [ [name] | [glob] | [regex] ] ... ]
show running-config pool
  show running-config pool [ [ [name] | [glob] | [regex] ] ... ]
  options:
    all-properties
    non-default-properties
    one-line
    partition
show pool
  show pool [name]
  options:
    all-properties
    (default | exa | gig | kil | meg | peta | raw | tera | yotta | zetta)
detail
  field-fmt

Delete
delete pool [name]

◆ Note
You must remove all references to a pool before you can delete the pool.
Description

You can use this pool component to configure the pool definitions on the Local Traffic Manager. A load balancing pool is a logical set of devices, such as Web servers, that you group together to receive and process traffic.

Examples

**create pool my_pool members add {**
  **  member 10.2.3.11:http**
  **  member 10.2.3.12:http**
  **}**

Creates a Local Traffic Manager pool named **my_pool** with two members, **10.2.3.11** and **10.2.3.12**, using the default values for the pool and pool members.

**delete pool my_pool**

Deletes the pool named **my_pool**.

**show pool**

Displays statistics and status for all Local Traffic Manager pools in the system configuration.

**show pool all-properties**

Displays statistics and status for all Local Traffic Manager pools in the system configuration.

Note that if the system includes Packet Velocity® ASIC (PVA) and PVA Assist capabilities, this command displays status and statistics for that feature.

**list pool my_pool**

Displays properties of the the pool named **my_pool**.

Options

- **all**
  Specifies that you want to modify all of the existing components of the specified type.

- **allow-nat**
  Specifies whether the pool can load balance network address translation (NAT) connections. The default value is **yes**.

- **allow-snat**
  Specifies whether the pool can load balance secure network address translation (SNAT) connections. The default value is **yes**.

- **description**
  User defined description.
◆ **gateway-failsafe-device**
   Specifies that the pool is a gateway failsafe pool in a redundant configuration. The gateway-failsafe-device identifies the device that depends on the gateway. If the monitor associated with the pool reports that the gateway is down, the device goes to the standby state. The default value for this string is empty, the feature is not configured.

◆ **glob**
   Displays the items that match the glob expression. See help glob for a description of glob expression syntax.

◆ **ignore-persisted-weight**
   Discounts the weight of connections made to pool members selected through persistence, rather than as a result of the algorithm configured on the pool. If the connection’s weight is ignored, then it is not treated as a ‘pick’ for that pool member, and does not influence subsequent pool member load balancing decisions.
   This option only impacts pools configured with one of the following load balancing modes: observed-member, observed-node, predictive-member, predictive-node, ratio-least-connections-member, ratio-least-connections-node, ratio-member, or ratio-node.
   The default value is no, which results in persisted pool member connections being accounted for during load balancing calculations.

◆ **ip-tos-to-client**
   Specifies the Type of Service (ToS) level to use when sending packets to a client. The default value is 65535 (pass-through).

◆ **ip-tos-to-server**
   Specifies the ToS level to use when sending packets to a server. The default value is 65535 (pass-through).

◆ **link-qos-to-client**
   Specifies the Link Quality of Service (QoS) level to use when sending packets to a client. The default value is 65535 (pass-through).

◆ **link-qos-to-server**
   Specifies the Link QoS level to use when sending packets to a server. The default value is 65535 (pass-through).

◆ **load-balancing-mode**
   Specifies the modes that the system uses to load balance name resolution requests among the members of this pool. The default value is round-robin.
   The options are:
   - **dynamic-ratio-member**
     Specifies that the system distributes connections based on various aspects of real-time server performance analysis, such as the number of current connections per node or the fastest node response time.
     This mode is similar to the dynamic-ratio-node mode, except that weights are based on continuous monitoring of the servers and are therefore continually changing.
• **dynamic-ratio-node**
  Specifies that the system distributes connections based on various aspects of real-time server performance analysis, such as the number of current connections per node or the fastest node response time. This mode is similar to the **dynamic-ratio-member** mode, except that weights are based on continuous monitoring of the servers and are therefore continually changing.

• **fastest-app-response**
  Specifies that the system passes a new connection based on the fastest response of all currently active nodes in a pool. This mode might be particularly useful in environments where nodes are distributed across different logical networks.

• **fastest-node**
  Specifies that the system passes a new connection based on the fastest response of all pools of which a server is a member. This mode might be particularly useful in environments where nodes are distributed across different logical networks.

• **least-connections-member**
  Specifies that the system passes a new connection to the node that has the least number of current connections in the pool. This mode works best in environments where the servers or other equipment you are load balancing have similar capabilities.
  This dynamic load balancing mode distributes connections based on various aspects of real-time server performance analysis, such as the current number of connections per node or the fastest node response time.

• **least-connections-node**
  Specifies that the system passes a new connection to the node that has the least number of current connections out of all pools of which a node is a member. This mode works best in environments where the servers or other equipment you are load balancing have similar capabilities.
  This dynamic load balancing mode distributes connections based on various aspects of real-time server performance analysis, such as the number of current connections per node, or the fastest node response time.

• **least-sessions**
  Specifies that the system passes a new connection to the node that has the least number of current sessions. This mode works best in environments where the servers or other equipment you are load balancing have similar capabilities.
  This dynamic load balancing mode distributes connections based on various aspects of real-time server performance analysis, such as the number of current sessions.

• **observed-member**
  Specifies that the system ranks nodes based on the number of connections. Nodes that have a better balance of fewest connections receive a greater proportion of the connections.
  This mode differs from the **least-connections-member** mode, which
measures connections only at the moment of load balancing, while the observed-member mode tracks the number of Layer 4 connections to each node over time and creates a ratio for load balancing. This dynamic load balancing mode works well in any environment, but may be particularly useful in environments where node performance varies significantly.

- **observed-node**
  Specifies that the system ranks nodes based on the number of connections. Nodes that have a better balance of fewest connections receive a greater proportion of the connections. This mode differs from least-connections-node mode, which measures connections only at the moment of load balancing, while the observed-node mode tracks the number of Layer 4 connections to each node over time and creates a ratio for load balancing. This dynamic load balancing method works well in any environment, but may be particularly useful in environments where node performance varies significantly.

- **predictive-member**
  Uses the ranking method used by the observed-member mode, except that the system analyzes the trend of the ranking over time, determining whether a node’s performance is improving or declining. The nodes in the pool with better performance rankings that are currently improving, rather than declining, receive a higher proportion of the connections. This dynamic load balancing mode works well in any environment.

- **predictive-node**
  Uses the ranking method used by the observed-node mode, except that the system analyzes the trend of the ranking over time, determining whether a node’s performance is improving or declining. The nodes in the pool with better performance rankings that are currently improving, rather than declining, receive a higher proportion of the connections. This dynamic load balancing mode works well in any environment.

- **ratio-least-connections-member**
  Specifies that the system weights connections to each pool member based on the value of the ratio weight defined for each pool member. If a ratio weight is unspecified, it will be treated as a default value of ‘1’.

- **ratio-least-connections-node**
  Specifies that the system weights connections to each pool member based on the value of the ratio weight defined for the pool member’s node. If a ratio weight is unspecified, it will be treated as a default value of ‘1’.

- **ratio-member**
  Specifies that the number of connections that each machine receives over time is proportionate to a ratio weight you define for each machine within the pool.
- **ratio-node**
  Specifies that the number of connections that each machine receives over time is proportionate to a ratio weight you define for each machine across all pools of which the server is a member.

- **ratio-session**
  Specifies that the number of sessions that each machine receives over time is proportionate to a ratio weight that you define for each machine within the pool.

- **round-robin**
  Specifies that the system passes each new connection request to the next server in line, eventually distributing connections evenly across the array of machines being load balanced. This mode works well in most configurations, especially if the equipment that you are load balancing is roughly equal in processing speed and memory.

- **weighted-least-connections-member**
  Specifies that the system passes a new connection to the pool member that is handling the lowest percentage of the specified maximum number of concurrent connections allowed. This mode works best in environments where the servers or other equipment you are load balancing have different but quantified capability limits. This mode requires that you specify a value for the **connection-limit** option for all members of the pool, but does not require all servers or other equipment you are load balancing to have similar capabilities.

- **weighted-least-connections-node**
  Specifies that the system passes a new connection to the node that is handling the lowest percentage of the specified connection limit. This mode works best in environments where the servers or other equipment you are load balancing have different but quantified capability limits. This mode requires that you specify a value for the **connection-limit** option for all nodes, but does not require all servers or other equipment you are load balancing to have similar capabilities.

- **members**
  Adds, deletes, or replaces a set of pool members, by specifying a node name and service port in the format `[node name/port]`. If a node by the specified name does not exist, it will be created. You can configure the following options for a pool member:

  - **address**
    Specifies the IP address of a pool member if a node by the name specified does not already exist.

  - **connection-limit**
    Specifies the maximum number of concurrent connections allowed for a pool member. The default value is 0 (zero).

  - **description**
    User defined description.
- **dynamic-ratio**
  Specifies a range of numbers that you want the system to use in conjunction with the ratio load balancing method. The default value is 1.

- **inherit-profile**
  Specifies whether the pool member inherits the encapsulation profile from the parent pool. The default value is enabled. If you disable inheritance, no encapsulation takes place, unless you specify another encapsulation profile for the pool member using the profiles attribute.

- **monitor**
  Specifies the health monitors that are configured to monitor the pool member. The default value is default, the system monitors the pool member using the monitors specified for the pool.

  You can specify:

  - A single monitor, for example, modify pool mypool members
    modify { pool_member_1:80 { monitor http } }.

  - Multiple monitors, for example, modify pool mypool members
    modify { pool_member_1:80 { monitor http and https } }.

  - A minimum number of monitors, for example, modify pool mypool
    members modify { pool_member_1:80 { monitor min 1 of { http https } } }.

  - No monitor rule or remove a monitor rule, for example, modify pool
    mypool members modify { pool_member_1:80 { monitor none } }.

- **profiles**
  Specifies the encapsulation profile to use for the pool member, when the inherit-profile attribute is disabled. The default value is none.

- **priority-group**
  Specifies the priority group within the pool for this pool member.
  Valid values are 0 through 65535. The system sends traffic to groups in order of priority. The default value is 1.

- **rate-limit**
  Specifies the maximum number of connections per second allowed for a pool member. The default value is ‘disabled’.

- **ratio**
  Specifies the weight of the pool member for load balancing purposes. The default value is 1.

- **session**
  Establishing a session with a pool member is establishing the ability of the client to persist to the pool member when making new connections. When a pool member is session disabled, clients that have already established sessions with the pool member may create new connections, but a client that has not already established a session may not create a new one (or make a connection which would create a new session). This feature is used to gently drain connections from a node, typically as part of a maintenance operation. The default value is user-enabled.

  The value of this property can be set by system or by user. If the value is set by system, the property will not be displayed in “Edit”
command. But, users can add this field in if they need to modify this property. The values which user can set for this property are user-enabled and user-disabled.

- **state**
  Marks the pool member user-up or user-down. The default value is user-up.

- **metadata**
  Associates user-defined data, each of which has name and value pair and persistence. The default value is persistent, which saves the data to the config file.

- **min-active-members**
  Specifies the minimum number of members that must be up for traffic to be confined to a priority group when using priority-based activation. The default value is 0 (zero). An active member is a member that is up (not marked down) and is handling fewer connections than its connection limit.

- **min-up-members**
  Specifies the minimum number of pool members that must be up; otherwise, the system takes the action specified in the min-up-members-action option.
  Use this option for gateway pools in a redundant system where a unit number is applied to the pool. This indicates that the pool is configured only on the specified unit.

- **min-up-members-action**
  Specifies the action to take if min-up-members-checking is enabled, and the number of active pool members falls below the number specified in the min-up-members option. The default value is failover. The options are:
  - **reboot**
    Specifies that when the min-up-members-checking option is enabled, and the number of active pool members is less than the number specified in the min-up-members option, the system restarts.
  - **restart-all**
    Specifies that when the min-up-members-checking option is enabled, and the number of active pool members is less than the number specified in the min-up-members option, the system restarts.
  - **failover**
    Specifies, for a redundant system, that when the min-up-members-checking option is enabled, and the number of active pool members is less than the number specified in the min-up-members option, the system fails over.

- **min-up-members-checking**
  Enables or disables the min-up-members feature. If you enable this feature, you must also specify a value for both the min-up-members and min-up-members-action options.

- **monitor**
  Specifies the health monitors that the system uses to determine whether it can use this pool for load balancing. The monitor marks the pool up or
down based on whether the monitor is successful. The default value is none.
You can specify:
• A single monitor, for example, **modify pool mypool monitor http**.
• Multiple monitors, for example, **modify pool mypool monitor http and https**.
• A minimum number of monitors, for example, **modify pool mypool monitor min 1 of {http and https}**.
• No monitor rule or remove a monitor rule, for example, **modify pool mypool monitor none**.

◆ **name**
Specifies a unique name for the component. This option is required for the commands **create**, **delete**, and **modify**.

◆ **partition**
Displays the administrative partition within which the pool resides.

◆ **profiles**
Specifies the profile to use for encapsulation. The default value is **none**, which indicates no encapsulation.

◆ **regex**
Displays the items that match the regular expression. The regular expression
must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. See **help regex** for a description of regular expression syntax.

◆ **reselect-tries**
When set to the default value of 0 (zero) the system does not attempt to load balance to another pool member after a passive failure. A passive failure is a pool member connection failure. When set to any other value, the system attempts to load balance to another pool member after a passive failure, and if that attempt also results in a passive failure, the system repeats the process until the specified number of reselection tries is reached.

◆ **reset-stats**
Resets the statistics for the specified component to 0 (zero).

◆ **service-down-action**
Specifies the action to take if the service specified in the pool is marked down. The options are:
• **drop**
  Specifies that the system drops connections when a the service is marked down.
• **none**
  Specifies that the system takes no action when a the service is marked down. This is the default value.
• **reselect**
  Specifies that the system reselects a node for the next packet that comes in on a Layer 4 connection, if the service of the existing connection is marked **down**.

• **reset**
  Specifies that the system resets when a the service is marked **down**.

• **slow-ramp-time**
  Specifies, in seconds, the ramp time for the pool. This provides the ability to cause a pool member that has just been **enabled**, or marked **up**, to receive proportionally less traffic than other members in the pool. The proportion of traffic the member accepts is determined by how long the member has been up in comparison to the value of the **slow-ramp-time** option for the pool.
  For example, if the **load-balancing-mode** of a pool is **round-robin** and it has a **slow-ramp-time** of 60 seconds, when a pool member has been up for only 30 seconds, the pool member receives approximately half the amount of new traffic as other pool members that have been up for more than 60 seconds. After the pool member has been up for 45 seconds, it receives approximately three quarters of the new traffic.
  The **slow-ramp-time** option is particularly useful when used with the **least-connections-member** load balancing mode. The default value is 10.

**See Also**

create, delete, edit, glob, list, modify, ltm virtual, regex, reset-stats, show, tmsh
Chapter 22

rule

Configures an iRule for traffic management system configuration.

Module

ltm

Syntax

Configure the rule component within the ltm module using the syntax shown in the following sections.

Create/Modify

create rule [name]
est edit rule [name]
modify rule [...] [...]

◆ Note

When using tmsh, you can only create iRules using the editor, which starts when you use the create, edit, or modify commands. You cannot create an iRule directly on the command line. The vim editor applies the autoindent and smartindent options. You can toggle on/off paste mode using the F12 key.

◆ Note

You can also edit the user metadata associated with an iRule. See the example section for more information.

Display

list rule
list rule [...] [...]
show running-config rule
show running-config rule [...] [...]
options:
  all-properties
  non-default-properties
show rule
show rule [...] [...]
options:
  (default | gig | kil | meg | raw)
  field-fmt
Delete

delete rule [name] description

Generate

generate rule [name]
options:
  checksum
  signature

Description

You cannot edit the system rules that come with the BIG-IP system. However, you can open a system rule in the editor and use it as a template to create a new rule.

To create a new rule using a system rule as a template

1. Enter the following command sequence:
   
   ```
   edit rule [system rule name]
   tmsh
   ```
   
   `tmsh` opens the system rule in the editor.

2. Change the name of the rule in the editor.

3. Edit the rule and exit the editor.
   
   ```
   tmsh
   ```
   
   `tmsh` checks for syntax errors, and if there are none, it saves the new rule.

For more information about iRules, see [http://devcentral.f5.com/](http://devcentral.f5.com/).

Examples

Displays all iRules:

```
list rule
```

Deletes the iRule named `my_irule`:

```
delete rule my_irule
```

Creates an iRule named `myRule`:

```
rule myRule {
    when RULE_INIT {
    }
    priority 1
    when SERVER_CONNECTED {
    }
    timing on
```
Generates a checksum for the rule definition and adds the checksum to the rule:

```bash
generate rule my_irule checksum
```

Generates a signature for the rule definition using the specified private key and adds the signature to the rule:

```bash
generate rule my_irule signature signing-key my_key
```

**Note**

For a rule that includes a checksum or signature to successfully load, the rule definition contents must match the stored checksum or signature. To modify the rule definition and still retain the checksum or signature, the `ignore-verification` attribute must be set to `true`. This is done by editing the rule and adding the `ignore-verification` attribute, which allows the modified rule to load and changes the verification status to **Not Verified**.

```bash
rule my_irule {
    when RULE_INIT {}
    definition-checksum 7c0dba9aa53e8959042c6cfe041d3d11
    ignore-verification true
}
```

Modifies an existing iRule named `my_irule` by adding a new metadata and modifying an existing metadata:

```bash
modify rule my_irule {
    when RULE_INIT {}
    definition-checksum 7c0dba9aa53e8959042c6cfe041d3d11
    metadata replace-all-with {
        my_meta {
            persist false
            value "hello"
        }
        my_meta2 {
            persist false
            value "hello 2"
        }
    }
}
```

The `metadata` attribute is the user defined key/value pair. Metadata has the following format:

```bash
metadata
    [add | delete | modify] {
    [metadata_name] {
```
Deletes a metadata from an iRule:

```bash
modify rule my_irule {
  when RULE_INIT {}
  definition-checksum 7c0dba9aa53e8959042c6cfe041d3d11
  metadata delete { my_meta }
}
```

## Options

You can use these options with the `rule` component:

- **checksum**
  Generates a checksum for the rule definition and add the checksum to the rule. This option is used only with the `generate` command.

- **glob**
  Displays the items that match the `glob` expression. For a description of `glob` expression syntax, see the `glob` man page.

- **name**
  Specifies a unique name for the component. This option is required for the `create`, `delete`, and `modify` commands.

- **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. For a description of regular expression syntax, see the `regex` man page.

- **signature**
  Generates a signature for the rule definition using the specified private key and adds the signature to the rule as a property. This option is used only with the `generate` command.

- **signing-key**
  Specifies the private key to use for signing the rule. This is used only with the `signature` option.

- **meta-data**
  Specifies the user-defined key/value pair associated with the rule. See the example section for usage format.

## See also

`create`, `delete`, `edit`, `generate`, `glob`, `list`, `modify`, `regex`, `show`, `tmsh`
snat

Configures secure network address translation (SNAT).

Module

ltm

Syntax

Configure the snat component within the ltm module using the following syntax.

Create/Modify

create snat [name]
modify snat [name]

options:
(automap | none)
auto-lasthop [default | enabled | disabled ]
description [string]
mirror {[disabled | enabled | none]}
origins
 [add | delete | replace-all-with] {
  [ip address ... ]
}
origins
 [add | delete | replace-all-with] {
  [address ... | address/mask ...]
}

snatpool [ name ]
source-port [change | preserve | preserve-strict ]
translation [translation name ... ]

vlans
 [add | delete | replace-all-with] {
  [vlan name ... ]
}
vlans [default | none]
[vlans-disabled | vlans-enabled]
metadata
 [add | delete | modify] {
  [metadata_name ... ] {
    value [ "value content" ]
    persist [ true | false ]
  }
}

}
edit snat [ [ [name] | [glob] | [regex] ] ... ]
  
  options:
  all-properties
  non-default-properties

Display

  list snat
  list snat [ [ [name] | [glob] | [regex] ] ... ]
  
  show running-config snat
  show running-config snat [ [ [name] | [glob] | [regex] ] ... ]
  
  options:
  all-properties
  non-default-properties
  one-line
  show snat
  show snat [ [ [name] | [glob] | [regex] ] ... ]
  
  options:
  (default | gig | kil | meg | raw)
  detail
  field-fmt

Delete

  delete snat [name]

Description

You can use the snat component to configure a SNAT. A SNAT defines the relationship between an externally visible IP address, SNAT IP address, or translated address, and a group of internal IP addresses, or originating addresses, of individual servers at your site.

Examples

Creates the SNAT my_snat that translates the address of connections that originate from the address 10.1.1.3 to the translation address mySnatTranslation:

<create snat my_snat origins add { 10.1.1.3 } translation mySnatTranslation>

Displays all properties for all SNATs:

list snat all-properties
Options

You can use these options with the **snat** component:

- **automap**
  Specifies that the system translates the source IP address to an available self IP address when establishing connections through the virtual server. You can use this option only if you do not use the **snatpool** and **translation** options.

  *Note:* When you use the *edit* command to create a new snat, by default the automap feature is enabled. If you do not want to use automap, you must turn the feature off by using the **none** option.

- **description**
  User-defined description.

- **glob**
  Displays the items that match the **glob** expression. For a description of **glob** expression syntax, see the **glob** man page.

- **mirror**
  Enables or disables mirroring of SNAT connections. The default value is **none**.

- **name**
  Specifies a unique name for the component. This option is required for the commands **create**, **delete**, and **modify**.

- **origins**
  Specifies a set of IP addresses and subnets from which connections originate. This option is required.

- **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. For a description of regular expression syntax, see the **regex** man page.

- **snatpool**
  Specifies the name of a SNAT pool. You can use this option only if you do not use the **automap** and **translation** options.

- **source-port**
  Specifies whether the system preserves the source port of the connection. The default value is **preserve**.

  The options are:
  - **change**
    Specifies that the system obfuscates internal network addresses.
  - **preserve**
    Specifies that the system preserves the source port of the connection.
  - **preserve-strict**
    Specifies that the system preserves the source port of the connection. Use this value for UDP only under very special circumstances, such as nPath or transparent (that is, no translation of any other L3/L4
field), where there is a one-to-one relationship between virtual IP addresses and node addresses, or when clustered multi-processing (CMP) is disabled.

- **translation**
  Specifies the name of a translated IP address. You can use this option only if you do not use the `automap` and `snatpool` options.
  
  *Note:* Translated addresses are outside the traffic management system.

- **vlans**
  Specifies the name of the VLAN to which you want to assign the SNAT. The default value is `none`.

- **vlans-disabled**
  Disables the SNAT on all VLANs. This is the default value.

- **vlans-enabled**
  Enables the SNAT on all VLANs.

- **metadata**
  Associates user-defined data, each of which has a name and value pair and persistence. The default value is `persistent`, which saves the data to the config file.

### See also

- `create`, `delete`, `edit`, `glob`, `list`, `ltm snat-translation`, `ltm snatpool`, `ltm vlan`, `modify`, `regex`, `show`, `tmsh`
Chapter 22

**snatpool**

Configures a secure network address translation (SNAT) pool.

**Module**

ltm

**Syntax**

Configure the **snatpool** component within the **ltm** module using the following syntax.

**Create/Modify**

create snatpool [name]
modify snatpool [name]

options:
  description [string]
  members
    [add | delete | replace-all-with] {
    [ip address ... ]
  }
  members [default | none]

edit snatpool [ [ [name] | [glob] | [regex] ] ... ]

options:
  all-properties
  non-default-properties
reset-stats snatpool
reset-stats snatpool [ [ [name] | [glob] | [regex] ] ... ]

**Display**

list snatpool
list snatpool [ [ [name] | [glob] | [regex] ] ... ]
show running-config snatpool
show running-config snatpool [ [ [name] | [glob] | [regex] ] ... ]

options:
  all-properties
  non-default-properties
  one-line
show snatpool
show snatpool [ [ [name] | [glob] | [regex] ] ... ]

options:
  (default | gig | kil | meg | raw)
Delete

```bash
delete snatpool [name]
```

Description

A **SNAT pool** is a pool of translation addresses that you can map to one or more original IP addresses. Translation addresses in a SNAT pool are not self IP addresses. You can simply create a SNAT pool and then assign it as a resource directly to a virtual server. This eliminates the need for you to explicitly define original IP addresses to which to map translation addresses.

Examples

Creates the SNAT pool `my_snat_pool1` that contains the translation addresses (members) 11.12.11.24 and 11.12.11.25:

```bash
create snatpool my_snat_pool1 members add { 11.12.11.24 11.12.11.25 }
```

Deletes the SNAT pool named `my_snat_pool1`:

```bash
delete snatpool my_snat_pool1
```

Options

You can use these options with the `snatpool` component:

- **description**
  
  User-defined description.

- **glob**
  
  Displays the items that match the `glob` expression. For a description of `glob` expression syntax, see the `glob` man page.

- **members**
  
  Specifies translation IP addresses of the pools in the SNAT pool.

- **name**
  
  Specifies a unique name for the component. This option is required.

- **regex**
  
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. For a description of regular expression syntax, see the `regex` man page.
See also

create, delete, edit, glob, list, ltm snat, ltm snat-translation, modify, regex, reset-stats, show, tmsh
snat-translation

Configures an explicit secure network address translation (SNAT) translation address.

Module

ltm

Syntax

Configure the snat-translation component within the ltm module using the following syntax.

Create/Modify

create snat-translation [all | [name] ]
modify snat-translation [all | [name] ]
   options:
         address [ip address]
         arp [disabled | enabled]
         connection-limit [integer]
         description [string]
         [disabled | enabled]
         ip-idle-timeout [indefinite | [integer] ]
         tcp-idle-timeout [indefinite | [integer] ]
         udp-idle-timeout [indefinite | [integer] ]
         traffic-group [string]
edit snat-translation [ [ [name] | [glob] | [regex] ] ... ]
   options:
         all-properties
         non-default-properties

Display

list snat-translation
list snat-translation [ [ [name] | [glob] | [regex] ] ... ]
show running-config snat-translation
show running-config snat-translation [ [ [name] | [glob] | [regex] ] ... ]
   options:
         all-properties
         non-default-properties
show snat-translation
show snat-translation [ [name] | [glob] | [regex] ] ...

options:
  (default | gig | kil | meg | raw)
  field-fmt

Delete

delete snat-translation [all | [name] ]

Description

Explicitly defines the properties of a SNAT translation address.

Examples

Disables Address Resolution Protocol (ARP) on all SNAT translation addresses:
modify snat-translation all arp disabled

Displays all properties of all SNAT translation addresses:
list snat-translation all-properties

Options

You can use these options with the snat-translation command:

◆ address
  The translation IP address.

◆ arp
  Indicates whether the system responds to ARP requests or sends gratuitous ARPs. The default value is enabled.

◆ connection-limit
  Specifies the number of connections a translation address must reach before it no longer initiates a connection. The default value of 0 indicates that the option is disabled.

◆ description
  User-defined description.

◆ disabled
  Disables SNAT translation.

◆ enabled
  Enables SNAT translation. The default value is enabled.

◆ glob
  Displays the items that match the glob expression. For a description of glob expression syntax, see the glob man page.
◆ **ip-idle-timeout**
   Specifies the number of seconds that IP connections initiated using a SNAT address are allowed to remain idle before being automatically disconnected. The default value is *indefinite*.

◆ **regex**
   Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. For a description of regular expression syntax, see the *regex* man page.

◆ **tcp-idle-timeout**
   Specifies the number of seconds that TCP connections initiated using a SNAT address are allowed to remain idle before being automatically disconnected. The default value is *indefinite*.

◆ **udp-idle-timeout**
   Specifies the number of seconds that UDP connections initiated using a SNAT address are allowed to remain idle before being automatically disconnected. The default value is *indefinite*.

◆ **unit**
   Read-only property that specifies the unit in a redundant system. Derived from *traffic-group*.

◆ **traffic-group**
   Specifies the traffic group of the failover device group on which the SNAT is active. The default traffic group is inherited from the containing folder.

◆ **inherited-traffic-group**
   Read-only property that indicates if the *traffic-group* is inherited from the parent folder.

**See also**

create, delete, edit, glob, list, ltm snat, ltm snatpool, modify, regex, show, tmsh
tce-policy

Configures TCE policies for the Local Traffic Manager.

Module

ltm

Syntax

Configure the tce-policy component within the ltm module using the syntax shown in the following sections.

Create/Modify

create tce-policy [name]
mody tce-policy [name]
options:
description [string]
tce-rule [add | delete | modify | none | replace-all-with] {
    [ [rule_name] ] {
options:
category [category_name]
description [string]
protocol [protocol_name]
steering [steering_name]
}
}
edit tce-policy [ [ [name] ] [ [glob] ] [ [regex] ] ... ]
options:
all-properties
non-default-properties
reset-stats tce-policy
reset-stats tce-policy [ [ [name] ] [ [glob] ] [ [regex] ] ... ]

Display

list tce-policy
list tce-policy [ [ [name] ] [ [glob] ] [ [regex] ] ... ]
show running-config tce-policy
show running-config tce-policy [ [ [name] ] [ [glob] ] [ [regex] ] ... ]
options:
all-properties
non-default-properties
one-line
partition
show tce-policy
show tce-policy [name]
options:
  all-properties
    (default | exa | gig | kil | meg | peta | raw | tera | yotta | zetta)
detail
field-fmt

Delete

delete tce-policy [name]

◆ Note
You must remove all references to a tce-policy before you can delete the tce-policy.

Description

You can use this tce-policy component to configure the TCE policy definitions on the Local Traffic Manager.

Examples

Creates a Local Traffic Manager tce-policy named my_policy with two tce-rules: my_rule_1 and my_rule_2. my_rule_1 defines the matching (category, protocol) to be (P2P, bittorrent) and steering action defined by my_endpoint_1, my_rule_1, and my_rule_2. my_rule_2 defines the matching (category, protocol) to be (web, all) and steering action defined by my_endpoint_2.

create tce-policy my_policy tce-rule add {
  my_rule_1 {
    category P2P
    protocol skype
    steering my_endpoint_1
  }
  my_rule_2 {
    category web
    protocol http
    steering my_endpoint_2
  }
}

Deletes the tce-policy named my_policy:
delete tce-policy my_policy

Displays statistics and status for all Local Traffic Manager tce-policies in the system configuration:

show tce-policy

Displays statistics and status for all Local Traffic Manager tce-policies in the system configuration:

show tce-policy all-properties

Displays properties of the tce-policy named my_policy:

list tce-policy my_policy

**Options**

- **category**
  Specifies the matching category.
- **description**
  User-defined description.
- **protocol**
  Specifies the matching protocol.
- **steering**
  Specifies the steering endpoint.

**See Also**

create, delete, edit, glob, list, modify, ltm steering-point, regex, reset-stats, show, tmsh
traffic-class

Configures a traffic class.

Module

ltm

Syntax

Configure the traffic-class component within the ltm module using the following syntax.

Create/Modify

create traffic-class [name]
modify traffic-class [name]

options:
  classification [string]
  description [string]
  destination-address [ [ip address] | none]
  destination-mask [ [ip address] | none]
  destination-port [ [integer] | [port name] ]
  protocol [any | [protocol] ]
  source-address [ [ip address] | none]
  source-mask [ [ip address] | none]
  source-port [ [integer] | [port name] ]

edit traffic-class [ [ [name] | [glob] | [regex] ] ... ]

options:
  all-properties
  non-default-properties
  one-line

Display

list traffic-class
list traffic-class [ [ [name] | [glob] | [regex] ] ... ]

show running-config traffic-class
show running-config traffic-class [ [ [name] | [glob] | [regex] ] ... ]

options:
  all-properties
  non-default-properties
  one-line
Chapter 22

Delete

delte traffic-class \[name\]

Description

You can use the `traffic-class` component to configure a traffic class, which is a named group of ports, machines, and subnets. You can then assign this traffic class to a virtual server to configure the virtual server to achieve specific Quality of Service (QoS) standards.

Examples

Creates a traffic class named `my_traffic_class`, which tags matching flows with My traffic class:

```
create traffic-class my_traffic_class classification "My traffic class"
```

Displays all of the properties of all of the traffic classes:

```
list traffic-class all-properties
```

Deletes the traffic class named `my_traffic_class`:

```
delete traffic-class my_traffic_class
```

Options

You can use these options with the `traffic-class` component:

- **classification**
  Specifies the actual textual tag to be associated with the flow, if the traffic class is matched. This option is required.

- **description**
  User-defined description.

- **destination-address**
  Specifies destination IP addresses for the system to use when evaluating traffic flow. If traffic flow matches this value, it is tagged with the value in the `classification` option. The default value is `none`.

- **destination-mask**
  Specifies a destination IP address mask for the system to use when evaluating traffic flow. If traffic flow matches this value, it is tagged with the value in the `classification` option. The default value is `none`.

- **destination-port**
  Specifies a destination port for the system to use when evaluating traffic flow. If traffic flow matches this value, it is tagged with the value in the `classification` option. The default value is `0` (zero).

- **glob**
  Displays the items that match the `glob` expression. For a description of `glob` expression syntax, see the `glob` man page.
◆ **name**
   Specifies a unique name for the component. This option is required for the commands `create`, `delete`, and `modify`.

◆ **protocol**
   Specifies a protocol for the system to use when evaluating traffic flow. If traffic flow matches this value, it is tagged with the value in the `classification` option. The default value is `any`.

◆ **regex**
   Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. For a description of regular expression syntax, see the `regex` man page.

◆ **source-address**
   Specifies source IP addresses for the system to use when evaluating traffic flow. If traffic flow matches this value, it is tagged with the value in the `classification` option. The default value is `none`.

◆ **source-mask**
   Specifies a source IP address mask for the system to use when evaluating traffic flow. If traffic flow matches this value, it is tagged with the value in the `classification` option. The default value is `none`.

◆ **source-port**
   Specifies a source port for the system to use when evaluating traffic flow. If traffic flow matches this value, it is tagged with the value in the `classification` option. The default value is `0` (zero).

**See also**

create, delete, edit, glob, list, ltm virtual, modify, regex, tmsh
virtual

Configures a virtual server.

Module

ltm

Syntax

Configure the virtual component within the ltm module using the syntax shown in the following sections.

Create/Modify

create virtual [name]
modify virtual [name]

options:

all
auth [add | delete | replace-all-with] {
   [profile_name ... ]
}
auth [default | none]
auto-lasthop [default | enabled | disabled]
clone-pools [add | delete | replace-all-with] {
   [pool_name ... ] {
      context [clientside | serverside]
   }
} clone-pools none
cmp-enabled [yes | no]
connection-limit [integer]
dhcp-relay
description [string]
destination [virtual_address_name:port]
   [disabled | enabled]
fallback-persistence [none | [profile name] ]
http-class none
http-class {
   [profile_name ... ]
}
ip-forward
ip-protocol [any | [protocol]
12-forward
last-hop-pool [ [pool_name] | none]
mask [ip address]
mirror { [disabled | enabled | none] }
nat64 [enabled | disabled]
persist [replace-all-with] {
   [profile_name ... ] {
      default [no | yes]
   }
} persist none
pool { [pool_name] | none}
profiles [add | delete | replace-all-with] {
  [profile_name ...] {
    context [all | clientside | serverside]
  }
}
profiles [default | none]
rate-class [name]
rate-limit [integer]
rate-limit-mode [destination | object | object-destination | object-source | object-source-destination | source | source-destination]
rate-limit-dst [integer]
rate-limit-src [integer]
reject
rules { [none | [rule_name ...] }
snat [automap | none]
snatpool [snatpool_name]
source-port [change | preserve | preserve-strict]
traffic-classes [add | delete | replace-all-with] {
  [traffic_class_name ...]
}
traffic-classes [default | none]
translate-address [enabled | disabled]
translate-port [enabled | disabled]
vlans [add | delete | replace-all-with] {
  [vlan_name ...]
}
vlans [default | none]
vlans-disabled
vlans-enabled
metadata [add | delete | modify] {
  [metadata_name ...] {
    value ["value content"]
    persist [true | false]
  }
}
reset-stats virtual [ [name] | [glob] | [regex] ] ...

Display
list virtual
  list virtual [ [name] | [glob] | [regex] ] ...
show running-config virtual
  show running-config virtual [ [name] | [glob] | [regex] ] ...
options:
  all-properties
  non-default-properties
  one-line
  partition
show virtual
  show virtual [ [name] | [glob] | [regex] ] ...
options:
  all-properties (default | exa | gig | kil | meg | peta | raw | tera | yotta | zetta)
detail
  field-fmt

Delete
delete virtual [name]
Description

You can use the virtual component to create, delete, modify properties on, and display information about virtual servers. Virtual servers are externally visible IP addresses that receive client requests. Rather than sending the requests directly to the destination IP address specified in the packet header, it sends the requests to any of several content servers that make up a load balancing pool. Virtual servers also apply various behavioral settings to multiple traffic types, enable persistence for multiple traffic types, and direct traffic according to user-written iRules™.

◆ Note

After you configure a Global Traffic Manager listener, when you use the tab completion feature within the ltm module, the listener displays as one of the virtual servers in the Configuration Items section.

Examples

create virtual myV2 { destination 11.11.11.12: any persist replace-all-with { source_addr } } pool myPool

Creates a virtual server named myV2, which uses the source address persistence method.

modify virtual vs_f14_http4 profiles replace-all-with { profile-udp }

Replaces the profile associated with the virtual server vs_f14_http4.

◆ Note

To replace the profile associated with a virtual server, you must enclose the name of the new profile in curly brackets.

delete virtual myV4 myV5 myV6

Deletes the virtual servers named myV4, myV5, and myV6.

show virtual myV4

Displays statistics and status for the virtual named myV4.

show virtual myV4 all-properties

Displays statistics and status for the virtual named myV4.

◆ Note

If the system includes Packet Velocity® ASIC (PVA) and PVA Assist capabilities, this command displays status and statistics for that feature.
Options

- **all**
  Specifies that you want to modify all of the existing components of the specified type.

- **auth**
  Specifies a list of authentication profile names, separated by spaces, that the virtual server uses to manage authentication.

- **clone-pools**
  Specifies a pool or list of pools that the virtual server uses to replicate either client or server traffic. You must specify a value of either `clientside` or `serverside` for the `context` option for each clone pool. Typically, this option is used for intrusion detection.

- **cmp-enabled**
  Enables or disables clustered multi-processor (CMP) acceleration. This feature applies to certain platforms only. The default value is `yes`.

- **connection-limit**
  Specifies the maximum number of concurrent connections you want to allow for the virtual server. The default value of 0 (zero) allows for an unlimited number of concurrent connections.

- **context**
  Specifies that the pool is either a `clientside` or `serverside` clone pool.

**Note**

`Because validation occurs outside of TMSH, you will receive an error when you modify the context for profiles in a virtual server.`

- **dhcp-relay**
  Specifies a virtual server that relays all received dhcp requests to all pool members. If there is no pool, the received request get dropped. If you specify the `dhcp-relay` option, you cannot use the `ip-forward` or `l2-forward` or `reject` options.

- **description**
  User defined description.

- **destination**
  Specifies the name of the virtual address and service on which the virtual server listens for connections. The default value is `any:any`.

- **(enabled | disabled)**
  Specifies the state of the virtual server. The default value is `enabled`.

**Note**

`When you disable a virtual server, the virtual server no longer accepts new connection requests. However, it allows current connections to finish processing before going to a `down` state.`

- **fallback-persistence**
  Specifies a fallback persistence profile for the virtual server to use when the default persistence profile is not available. The default value is `none`.
◆ glob
Displays the items that match the glob expression. See help glob for a description of glob expression syntax.

◆ http-class
Specifies a list of HTTP class profiles, separated by spaces, with which the virtual server works to increase the speed at which the virtual server processes HTTP requests. The default value is none. The order in which the profiles are entered sets the priority of each profile, in ascending order, specific to this virtual server.

◆ ip-forward
Specifies a virtual server that has no pool members to load balance, but instead, forwards the packet directly to the destination IP address specified in the client request. If you specify the ip-forward option, you cannot use the l2-forward or reject options.

◆ ip-protocol
Specifies the IP protocol for which you want the virtual server to direct traffic. Sample protocol names are TCP and UDP. The default value is any.

◆ Note
You do not use this setting when creating an HTTP class virtual server.

◆ l2-forward
Specifies a virtual server that shares the same IP address as a node in an associated VLAN. You create this type of virtual server when you want to create a VLAN group. If you specify the l2-forward option, you cannot use the ip-forward or reject options.

◆ last-hop-pool
Specifies the name of the last hop pool that you want the virtual server to use to direct reply traffic to the last hop router. The default value is none.

◆ mask
Specifies the netmask for a network virtual server only. This setting is required for a network virtual server.
The netmask clarifies whether the host bit is an actual zero or a wildcard representation. The default value is 255.255.255.255.

◆ mirror
Enables or disables mirroring. You can use mirroring to maintain the same state information in the standby unit that is in the active unit, allowing transactions such as FTP file transfers to continue as though uninterrupted. The default value is none.

◆ name
Specifies a unique name for the component. This option is required for the commands create, delete, and modify.

◆ nat64
Enable or disable NAT64. The default value is disabled. NAT64 is a service that automatically translate IPv6 traffic into IPv4.
- **partition**
  Displays the name of the administrative partition within which the virtual server resides.

- **persist**
  Specifies a list of profiles separated by spaces that the virtual server uses to manage connection persistence. The default value is `none`. To enable persistence, typically you specify a single profile. However, you can specify multiple profiles in conjunction with iRules™ that define a persistence strategy based on incoming traffic. In the case of multiple profiles, the `default` option specifies which profile you want the virtual server to use if an iRule does not specify a persistence method. When you specify multiple profiles, the default value of the default property is `no`. You can set the value of the `default` property to `yes` for only one of the profiles.

- **pool**
  Specifies a default pool to which you want the virtual server to automatically direct traffic. The default value is `none`.

- **profiles**
  Specifies a list of profiles for the virtual server to use to direct and manage traffic. The default value is `fastL4`.

- **rate-class**
  Specifies the name of an existing rate class that you want the virtual server to use to enforce a throughput policy for incoming network traffic. The default value is `none`.

- **rate-limit**
  Specifies the maximum number of connections per second allowed for a virtual server. The default value is ‘disabled’.

- **rate-limit-mode**
  Indicates whether the rate limit is applied per virtual object, per source address, per destination address, or some combination thereof. The default value is ‘object’, which does not use the source or destination address as part of the key.

- **rate-limit-dst-mask**
  Specifies a mask, in bits, to be applied to the destination address as part of the rate limiting. The default value is ‘0’, which is equivalent to using the entire address - ‘32’ in IPv4, or ‘128’ in IPv6.

- **rate-limit-src-mask**
  Specifies a mask, in bits, to be applied to the source address as part of the rate limiting. The default value is ‘0’, which is equivalent to using the entire address - ‘32’ in IPv4, or ‘128’ in IPv6.

- **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that
the identifier is a regular expression. See help regex for a description of regular expression syntax.

◆ reject
   Specifies that the BIG-IP® system rejects any traffic destined for the virtual server IP address. If you specify the reject option, you cannot use the ip-forward or l2-forward options.

◆ rules
   Specifies a list of iRules, separated by spaces, that customize the virtual server to direct and manage traffic. The default value is none.

◆ snat
   Specifies whether SNAT automap is enabled for the virtual server. The default value is none.

◆ snatpool
   Specifies the name of an existing SNAT pool that you want the virtual server to use to implement selective and intelligent SNATs.

◆ source-port
   Specifies whether the system preserves the source port of the connection. The default value is preserve. The options are:
   • change
     Obfuscates internal network addresses.
   • preserve
     Preserves the source port of the connection.
   • preserve-strict
     Use this value only for UDP under very special circumstances, such as nPath or transparent (that is, no translation of any other L3/L4 field), where there is a 1:1 relationship between virtual IP addresses and node addresses, or when clustered multi-processing (CMP) is disabled.

◆ traffic-classes
   Specifies a list of traffic classes that are associated with the virtual server. The default value is none.

◆ translate-address
   Enables or disables address translation for the virtual server. Disable address translation for a virtual server if you want to use the virtual server to load balance connections to any address. This option is useful when the system is load balancing devices that have the same IP address. The default value is disabled.

◆ translate-port
   Enables or disables port translation. Disable port translation for a virtual server, if you want to use the virtual server to load balance connections to any service. The default value is disabled.

◆ vlans
   Specifies a list of VLANs on which the virtual server is either enabled or disabled. The default value is none. The options
vlans-disabled and vlans-enabled indicate whether the virtual server is disabled or enabled on the list of specified VLANs.

- vlans-disabled
  Disables the virtual server on the VLANs specified in the vlans option. This is the default setting.

- vlans-enabled
  Enables the virtual server on the VLANs specified in the vlans option.

- metadata
  Associates user defined data, each of which has name and value pair and persistence. Persistent(default) means the data will be saved into config file.

See Also

create, delete, edit, glob, list, ltm persistence, ltm pool, modify, net vlan, net vlantage, regex, reset-stats, rule, show, tmsh
virtual-address

Configures virtual addresses.

Module

ltm

Syntax

Configure the virtual-address component within the ltm module using the following syntax.

Create/Modify

create virtual address [name]
modify virtual address [name]
options:
    address [ip address]
    arp [enabled | disabled]
    connection-limit [integer]
    description [string]
    enabled [yes | no]
    floating [enabled | disabled]
    mask [netmask]
    route-advertisement [enabled | disabled]
    server-scope [all | any | none]
    traffic-group [string]
    metadata
        [add | delete | modify] {
            [metadata_name ... ] {
                value [ "value content" ]
                persist [ true | false ]
            }
        }
    
edit virtual-address [ [ [name] | [glob] | [regex] ] ... ]
    options:
        all-properties
        non-default-properties
reset-stats virtual-address
reset-stats virtual-address [ [ [name] | [glob] | [regex] ] ... ]
Display

list virtual-address
list virtual-address [ [name] | [glob] | [regex] ] ...
show running-config virtual-address
show running-config virtual-address [ [name] | [glob] | [regex] ] ...

options:
  all-properties
  non-default-properties
  one-line
  partition

show virtual-address
show virtual-address [name]

options:
  (default | gig | kil | meg | raw)
  detail
  field-fmt

Delete

delete virtual-address [name]

Description

You can use the virtual-address component to enable, disable, display, and delete virtual addresses. You can also list the virtual address configuration and view statistics for a specific virtual address.

◆ Note

tmsh only displays virtual addresses when you explicitly request them.

To display the properties of virtual addresses or a specific virtual address from the ltm module, use the command sequences list virtual-address and list virtual-address [name], respectively.

To display statistics for virtual addresses or a specific virtual address from the ltm module, use the command sequence show virtual-address and show virtual-address [name], respectively.

Examples

Creates a virtual address 10.10.10.20, with a name of myVirtualAddr:

create virtual-address myVirtualAddr address 10.10.10.20 enabled yes
Creates a virtual address 10.10.10.20, with a name of myVirtualAddr, that is assigned to traffic-group-1.

```
create virtual-address myVirtualAddr address 10.10.10.20 enabled yes traffic-group /Common/traffic-group-1
```

Disables the virtual address myVirtualAddr:
```
modify virtual-address myVirtualAddr enabled no
```

Deletes the virtual address myVirtualAddr:
```
delete virtual-address myVirtualAddr
```

Lists the configuration information for the virtual address, myVirtualAddr:
```
list virtual-address myVirtualAddr all-properties
```

Displays statistics and status for the virtual-address myVirtualAddr:
```
show virtual-address myVirtualAddr
```

Displays statistics and status for the virtual named myVirtualAddr:
```
<show virtual-address myVirtualAddr all-properties
```

**Note**

If the system includes Packet Velocity, ASIC (PVA), and PVA Assist capabilities, this command displays status and statistics for that feature.

**Options**

You can use these options with the virtual-address component:

- **address**
  The virtual IP address.

- **arp**
  Enables or disables ARP for the specified virtual address. The default value is `enabled`.

- **description**
  User-defined description.

- **connection-limit**
  Sets a concurrent connection limit in seconds for one or more virtual servers. The default value is 0 seconds.

- **enabled**
  Specifies whether the specified virtual address is enabled. The default value is `yes`.

- **floating**
  Read-only property derived from traffic-group. A floating virtual address is a virtual address for a VLAN that serves as a shared address by all devices of a BIG-IP traffic-group.

- **glob**
  Displays the items that match the glob expression. For a description of glob expression syntax, see the glob man page.
◆ **mask**  
Sets the netmask for one or more network virtual servers only. This option is required for network virtual servers. The default value is 255.255.255.255.

◆ **partition**  
Displays the administrative partition within which the virtual address resides.

◆ **regex**  
Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. For a description of regular expression syntax, see the `regex` man page.

◆ **route-advertisement**  
Enables or disables route advertisement for the specified virtual address. The default value is disabled.

◆ **server-scope**  
Specifies the server that uses the specified virtual address. The default value is any.

◆ **unit**  
Read-only property that specifies the unit in a redundant system. Based on `traffic-group`.

◆ **traffic-group**  
Specifies the traffic group on which the virtual address is active. The default traffic group is inherited from the containing folder.

◆ **inherited-traffic-group**  
Read-only property that indicates if the `traffic-group` is inherited from the parent folder.

◆ **metadata**  
Associates user-defined data, each of which has a name-value pair and persistence. The default value is persistent, which saves the data to the config file.

**See also**

create, delete, edit, glob, list, ltm virtual, modify, regex, reset-stats, show, tmsh
Introducing the Ltm auth module

Alphabetical list of components
Introducing the ltm auth module

You can use the tmsh components that reside within the ltm auth module to configure profiles for Local Traffic Manager™. For more information about the tmsh hierarchical structure, see Chapter 2, Understanding and Using the Traffic Management Shell.

Alphabetical list of components

The remainder of this chapter lists the tmsh components that are available in the ltm auth module.
crldp-server

Configures a Certificate Revocation List Distribution Point (CRLDP) server for implementing CRLDP authentication.

Module

ltm auth

Syntax

Configure the crldp-server component within the ltm auth module using the following syntax.

Create/Modify

create crldp-server [name]
modify crldp-server [name]
  options:
   base-dn [ [LDAP base directory name] | none]
   host [ [ip address] | none]
   port [ [name] | [number] ]
   reverse-dn [disabled | enabled]
edit crldp-server [ [ [name] | [glob] | [regex] ] ... ]
  options:
   all-properties
   non-default-properties

Display

list crldp-server
list crldp-server [ [ [name] | [glob] | [regex] ] ... ]
show running-config crldp-server
show running-config crldp-server [ [ [name] | [glob] | [regex] ] ... ]
  options:
   all-properties
   non-default-properties
   one-line
   partition

Delete

delete crldp-server [name]
CRLDP authentication is a mechanism for checking certificate revocation status for client connections passing through the BIG-IP® system. This module is useful when your authentication data is stored on a remote CRLDP server.

**To implement a CRLDP authentication module and create a CRLDP server**

1. Use the `crldp-server` component in the `ltm auth` module to create a CRLDP server.
2. Use the `ssl-crldp` component in the `ltm auth` module to create a CRLDP configuration object and associate it with the server you created in Step 1.
3. Use the `profile` component in the `ltm auth` module to create an authentication profile in which you specify the following two options:
   a) For the `configuration` option, specify the CRLDP configuration object that you created in Step 2.
   b) For the `defaults-from` option, specify a parent profile (either the default profile named `ssl_crldp` or another custom profile that you created).

**Examples**

Creates a CRLDP server named `my_crldp_server`:

```
create crldp my_crldp_server
```

Deletes the CRLDP server named `my_crldp_server`:

```
delete crldp-server my_crldp_server
```

**Options**

You can use these options with the `crldp-server` component:

- **base-dn**
  Specifies the LDAP base directory name for certificates that specify the CRL distribution point in directory name format (dirName). The default value is `none`.
  
  Use this option when the value of the X.509v3 attribute `crlDistributionPoints` is of type `dirName`. In this case, the BIG-IP system attempts to match the value of the `crlDistributionPoints` attribute to the value of the `base-dn` option. An example of a `base-dn` value is `cn=lxxx,dc=f5,dc=com`.

- **description**
  User-defined description.
◆ **glob**
Displays the items that match the **glob** expression. For a description of glob expression syntax, see the **glob** man page.

◆ **host**
Specifies an IP address for the CRLDP server. This option is required. The default value is **none**.

◆ **name**
Specifies a unique name for the component. This option is required for the commands create, delete, and modify.

◆ **partition**
Displays the administrative partition within which the component resides.

◆ **port**
Specifies the port for CRLDP authentication traffic. The default value is **389**.

◆ **regex**
Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. For a description of regular expression syntax, see the **regex** man page.

◆ **reverse-dn**
Specifies in which order the system attempts to match the value of the **base-dn** option to the value of the X.509v3 attribute **crlDistributionPoints**. When **enabled**, the system matches the value of the **base-dn** option from left to right, or from the beginning of the DN string, to accommodate dirName strings in certificates such as C=US,ST=WA,L=SEA,OU=F5,CN=xxx. The default value is **disabled**.

**See also**
create, delete, edit, glob, list, ltm auth profile, ltm auth ssl-crldp, ltm virtual, modify, regex, reset-stats, show, tmsh
**kerberos-delegation**

Configures a Kerberos delegation profile.

**Module**

`ltm auth`

**Syntax**

Configure the `kerberos-delegation` component within the `ltm auth` module using the following syntax.

**Create/Modify**

- `create kerberos-delegation [name]`
- `modify kerberos-delegation [name]`
  - options:
    - client-principal [string]
    - debug-logging [disabled | enabled]
    - protocol-transition [disabled | enabled]
    - server-principal [string]
- `edit kerberos-delegation [ [name] | [glob] | [regex] ] ... ]`
  - options:
    - all-properties
    - non-default-properties
- `reset-stats kerberos-delegation`
- `reset-stats kerberos-delegation [ [name] | [glob] | [regex] ] ... ]`

**Display**

- `list kerberos-delegation`
- `list kerberos-delegation [ [name] | [glob] | [regex] ] ... ]`
- `show running-config kerberos-delegation`
- `show running-config kerberos-delegation [ [name] | [glob] | [regex] ] ... ]`
  - options:
    - all-properties
    - non-default-properties
    - one-line
    - partition
- `show kerberos-delegation`
show kerberos-delegation [ [ [name] | [glob] | [regex] ] ... ]

options:
(d [default | exa | gig | kil | meg | peta | raw | tera | yotta | zetta])
field-fmt
global

Delete

delete kerberos-delegation [name]

Description

The Kerberos delegation configuration acts like a proxy for Kerberos credentials. When connecting to a server that is inside its domain, the browser client fetches Kerberos credentials known as delegated credentials. These credentials are passed on to the system. Once the system has these credentials, it retrieves credentials for the Kerberos server that is on the back end and passes those credentials back.

Each user is assigned a unique cookie that describes a session on the system. This cookie is encrypted in a cookie key.

To configure a Kerberos authentication module and create a Kerberos configuration object

1. Use the kerberos-delegation component in the ltm auth module to create a Kerberos configuration object.
2. Use the profile component, in the ltm auth module, to create an authentication profile in which you specify the following two options:
   a) For the configuration option, specify the Kerberos configuration object that you created in Step 1.
   b) For the defaults-from option, specify a parent profile (either the default Kerberos profile named krbdelegate or another custom Kerberos profile that you created).

Examples

Creates a Kerberos delegation profile named my_kerberos-delegation_profile that inherits its settings from the system default Kerberos delegation profile named kerberos-delegation:

create kerberos-delegation my_kerberos-delegation_profile defaults-from \ kerberos-delegation

Displays all properties for all Kerberos delegation profiles:

list kerberos-delegation all-properties
Options

You can use the following options with the `kerberos-delegation` component:

- **client-principal**  
  Specifies the principal that the client sees. This is usually a value such as `HTTP/<fqdn>`. This principal can be in a different domain from the server principal. This option is required. There is no default value.

- **debug-logging**  
  Specifies whether the system logs debugging actions. The default value is disabled.

- **description**  
  User-defined description.

- **glob**  
  Displays the items that match the glob expression. For a description of glob expression syntax, see the glob man page.

- **name**  
  Specifies a unique name for the component. This option is required for the commands create, delete, and modify.

- **partition**  
  Displays the administrative partition within which the component resides.

- **protocol-transition**  
  Specifies whether associated virtual should transition client certificate authentication into Kerberos credentials.

- **regex**  
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (`@[regular expression]`) to indicate that the identifier is a regular expression. For a description of regular expression syntax, see the regex man page.

- **server-principal**  
  Specifies the principal of the back-end web server. This is usually a value such as `HTTP/<fqdn of server>`. This can be in a different domain from the server principal. This setting is required. There is no default value.

See also

create, delete, edit, glob, list, ltm virtual, modify, regex, reset-stats, show, tmsh
**ldap**

Configures an LDAP configuration object for implementing remote LDAP-based client authentication.

**Module**

*ltm auth*

**Syntax**

Configure the **ldap** component within the **ltm auth** module using the following syntax.

**Create/Modify**

```
create ldap [name]
modyify ldap [name]
```

**options:**

bind-dn [ [account dn] | none]
bind-pw [ [string] | none]
bind-timeout [integer]
check-host-attr [disabled | enabled]
description [string]
debug [disabled | enabled]
filter [ [string] | none]
group-dn [ [group dn] | none]
group-member-attr [ [string] | none]
idle-timeout [integer]
ignore-auth-info-unavail [no | yes]
ignore-unknown-user [disabled | enabled]
login-attribute [ [account name] | none]
port [ [name] | [integer] ]
scope [base | one | sub]
search-base-dn [ [search base dn] | none]
search-timeout [number]
servers [add | delete | replace-all-with] { [ip address ... ] }
servers none
ssl [disabled | enabled]
ssl-ca-cert-file [ [name] | none]
ssl-check-peer [disabled | enabled]
ssl-ciphers [ [string] | none]
ssl-client-cert [ [string] | none]
ssl-client-key [ [string] | none]```
user-template [ [string] | none]
version [number]
warnings [disabled | enabled]
edit ldap [ [ [name] | [glob] | [regex] ] ... ]
options:
  all-properties
  non-default-properties

Display

list ldap
list ldap [ [ [name] | [glob] | [regex] ] ... ]
show running-config ldap
show running-config ldap [ [ [name] | [glob] | [regex] ] ... ]
options:
  all-properties
  non-default-properties
  one-line
  partition

Delete

delete ldap [name]

Description

LDAP authentication is a mechanism for authenticating or authorizing client connections passing through the system. LDAP authentication is useful when your authentication or authorization data is stored on a remote LDAP server or a Microsoft® Windows® Active Directory® server, and you want the client credentials to be based on basic HTTP authentication (that is, user name and password).

To configure an LDAP authentication module and create an LDAP configuration object

1. Use the ldap component in the ltm auth module to create an LDAP configuration object.

2. Use the profile component in the ltm auth module to create an authentication profile in which you specify the following two options:

   a) For the configuration option, specify the LDAP configuration object that you created in Step 1.

   b) For the defaults-from option, specify a parent profile (either the default profile named ldap or another custom profile that you created).
Examples

Creates a configuration object named `my_auth_ldap`:

```
create ldap my_auth_ldap servers add {my_ldap_auth_server}
```

Deletes the configuration object named `my_auth_ldap`:

```
delete ldap my_auth_ldap
```

Options

You can use these options with the `ldap` component:

- **bind-dn**
  Specifies the distinguished name of an account to which to bind, to perform searches. This search account is a Read-only account used to do searches. You can use the `admin` account as the search account. If no admin DN is specified, then no bind is attempted. The default value is `none`.
  This option is required only when a site does not accept anonymous searches. If the remote server is a Microsoft Windows Active Directory server, the distinguished name must be in the form of an email address.

- **bind-pw**
  Specifies the password for the search account created on the LDAP server. This option is required if you specify a value for the `bind-dn` option. The default value is `none`.

- **bind-timeout**
  Specifies a bind timeout limit, in seconds. The default value is 30 seconds.

- **check-host-attr**
  Confirms the password for the bind distinguished name. This option is optional. The default value is `disabled`.

- **debug**
  Enables or disables `syslog-ng` debugging information at LOG DEBUG level. The default value is `disabled`. F5 Networks does not recommend using this option for normal configuration.

- **description**
  User-defined description.

- **filter**
  Specifies a filter. Use this option for authorizing client traffic. The default value is `none`.

- **glob**
  Displays the items that match the `glob` expression. For a description of `glob` expression syntax, see the `glob` man page.

- **group-dn**
  Specifies the group distinguished name. The system uses this option for authorizing client traffic. The default value is `none`.
- **group-member-attribute**
  Specifies a group member attribute. The system uses this option for authorizing client traffic. The default value is **none**.

- **idle-timeout**
  Specifies the idle timeout, in seconds, for connections. The default value is **3600** seconds.

- **ignore-auth-info-unavail**
  Specifies whether the system ignores authentication information, if it is not available. The default value is **no**.

- **ignore-unknown-user**
  Specifies whether the system ignores a user that is unknown. The default value is **disabled**.

- **name**
  Specifies a unique name for the component. This option is required for the commands **create**, **delete**, and **modify**.

- **login-attribute**
  Specifies a logon attribute. Normally, the value for this option is **uid**; however, if the server is a Microsoft Windows Active Directory server, the value must be the account name **samaccountname** (not case-sensitive). The default value is **none**.

- **partition**
  Displays the administrative partition within which the component resides.

- **port**
  Specifies the port number or name for the LDAP service. Port **389** is typically used for non-SSL and port **636** is used for an SSL-enabled LDAP service. The default value is **ldap**.

- **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. For a description of regular expression syntax, see the **regex** man page.

- **scope**
  Specifies the search scope. The default value is **sub**.
  The options are:
  - **base**
    Specifies the search scope is base object. The **base** value is almost never useful for nameservice lookups.
  - **one**
    Specifies the search scope is one level.
  - **sub**
    Specifies the search scope is subtree.

- **search-base-dn**
  Specifies the search base distinguished name. The default value is **none**.

- **search-timeout**
  Specifies the search timeout, in seconds. The default value is **30** seconds.
◆ servers
   Specifies the LDAP servers that the system must use to obtain authentication information. You must specify a server when you create an LDAP configuration object.

◆ ssl
   Enables or disables SSL. The default value is disabled.
   Note: When you use the command line interface to enable SSL for an LDAP service, the system does not change the service port number from 389 to 636, as is required. To change the port number, use the port option of this command, for example: ldap [name] ssl enabled port 636.

◆ ssl-ca-cert-file
   Specifies the name of an SSL CA certificate using the full path to the file. The default value is none.

◆ ssl-check-peer
   Specifies whether the system checks an SSL peer. The default value is disabled.

◆ ssl-ciphers
   Specifies SSL ciphers. The default value is none.

◆ ssl-client-cert
   Specifies the name of an SSL client certificate. The default value is none.

◆ ssl-client-key
   Specifies the name of an SSL client key. The default value is none.

◆ use-first-pass
   Specifies that the LDAP application tries the first password provided in the authentication stack, and then prompts for the user’s LDAP password if authentication fails. The default value is disabled.

◆ user-template
   Specifies a user template for the LDAP application to use for authentication. The default value is none.

◆ version
   Specifies the version number of the LDAP application. The default value is 3.

◆ warnings
   Enables or disables warning messages. The default value is enabled.

See also

create, delete, edit, glob, list, ltm auth profile, ltm virtual, modify, regex, reset-stats, show, tmsh
ocsp-responder

Configures Online Certificate System Protocol (OCSP) responder objects.

Module

ltm auth

Syntax

Configure the ocsp-responder component within the ltm auth module using the following syntax.

Create/Modify

create ocsp-responder [name]
modify ocsp-responder [name]

options:
  allow-certs [disabled | enabled]
  ca-file [ [file name] | none]
  ca-path [ [file name] | none]
  cert-id-digest [md5 | sha1]
  chain [disabled | enabled]
  description [string]
  check-certs [disabled | enabled]
  explicit [disabled | enabled]
  ignore-aia [disabled | enabled]
  intern [disabled | enabled]
  sign-digest [md5 | sha1]
  sign-key [ [key] | none]
  sign-key-pass-phrase [ [pass phrase] | none]
  sign-other [ list of certs ] | none]
  signer [ [certificate] | none]
  status-age [integer]
  trust-other [disabled | enabled]
  url [none | [url] ]
  va-file [ [file name] | none]
  validity-period [integer]
  verify [disabled | enabled]
  verify-cert [disabled | enabled]
  verify-other [ [file name] | none]
  verify-sig [disabled | enabled]
edit ocsp-responder [ [name] | [glob] | [regex] ] ... 
   options:
   all-properties
   non-default-properties

Display
list ocsp-responder
list ocsp-responder [ [name] | [glob] | [regex] ] ... 
show running-config ocsp-responder
show running-config ocsp-responder [ [name] | [glob] | [regex] ] ... 
   options:
   all-properties
   non-default-properties
   one-line
   partition

Delete
delete ocsp-responder [name]

Description
You can use the ocsp-responder component to configure Online Certificate System Protocol (OCSP) responder objects.

To implement an SSL OCSP authentication module and create an OCSP responder object

1. Use the ocsp-responder component in the ltm auth module to configure an OCSP responder object.

2. Use the ssl-ocsp component in the ltm auth module to configure an SSL OCSP configuration object to which you add the OCSP responder object that you created in Step 1.

3. Use the profile component in the ltm auth module to create an authentication profile in which you specify the following two options:
   a) For the configuration option, specify the SSL OCSP configuration object that you created in Step 2.
   b) For the defaults-from option, specify a parent profile (either the default OCSP Responder profile named ssl_ocsp or another custom profile that you created).
Options

You can use these options with the `ocsp-responder` component:

- **allow-certs**
  Enables or disables the addition of certificates to an OCSP request. The default value is **enabled**.

- **ca-file**
  Specifies the name of the file containing trusted CA certificates used to verify the signature on the OCSP response. The default value is **none**.

- **ca-path**
  Specifies the name of the path containing trusted CA certificates used to verify the signature on the OCSP response. The default value is **none**.

- **cert-id-digest**
  Specifies a specific algorithm identifier, either **sha1** or **md5**. The default value is **sha1**.
  The options are:
  - **sha1** is newer and provides more security with a 160-bit hash length.
  - **md5** is older and has only a 128-bit hash length.
  The cert ID is part of the OCSP protocol. The OCSP client (in this case, the BIG-IP system) calculates the cert ID using a hash of the Issuer and serial number for the certificate that it is trying to verify.

- **chain**
  Specifies whether the system constructs a chain from certificates in the OCSP response. The default value is **enabled**.

- **check-certs**
  Enables or disables verification of an OCSP response certificate. Use this option for debugging purposes only. The default value is **enabled**.

- **description**
  User-defined description.

- **explicit**
  Specifies that Local Traffic Manager™ explicitly trusts that the OCSP response signer's certificate is authorized for OCSP response signing. If the signer's certificate does not contain the OCSP signing extension, specification of this option causes a response to be untrusted. The default value is **enabled**.

- **glob**
  Displays the items that match the **glob** expression. For a description of **glob** expression syntax, see the **glob** man page.

- **ignore-aia**
  Specifies whether the system ignores the URL contained in the certificate's AIA fields and always uses the URL specified by the responder instead. The default value is **disabled**.
◆ **intern**
Specifies whether the system ignores certificates contained in an OCSP response when searching for the signer's certificate. To use this option, the signer's certificate must be specified with either the **verify-other** or **va-file** option. The default value is **enabled**.

◆ **name**
Specifies a unique name for the component. This option is required for the commands **create**, **delete**, and **modify**.

◆ **partition**
Displays the administrative partition within which the component resides.

◆ **regex**
Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. For a description of regular expression syntax, see the **regex** man page.

◆ **sign-digest**
Specifies the algorithm for signing the request, using the signing certificate and key. This parameter has no meaning, if request signing is not in effect (that is, both the request signing certificate and request signing key parameters are empty). This parameter is required only when request signing is in effect. The default value is **sha1**.

◆ **sign-key**
Specifies the key that the system uses to sign an OCSP request. The default value is **none**.

◆ **sign-key-pass-phrase**
Specifies the passphrase that the system uses to encrypt the sign key. The default value is **none**.

◆ **sign-other**
Adds a list of additional certificates to an OCSP request. The default value is **none**.

◆ **signer**
Specifies a certificate used to sign an OCSP request. If the certificate is specified, but the key is not specified, then the private key is read from the same file as the certificate. If neither the certificate nor the key is specified, then the request is not signed. If the certificate is not specified and the key is specified, then the configuration is considered to be invalid. The default value is **none**.

◆ **status-age**
Specifies the age of the status of the OCSP responder. The default value is 0 (zero).

◆ **trust-other**
Instructs the BIG-IP Local Traffic Manager system to trust the certificates specified with the **verify-other** option. The default value is **disabled**.

◆ **url**
Specifies the URL used to contact the OCSP service on the responder. This option is required. The default value is **none**.
◆ va-file
  Specifies the name of the file containing explicitly trusted responder certificates. This parameter is needed in the event that the responder is not covered by the certificates already loaded into the responder's CA store. The default value is none.

◆ validity-period
  Specifies the number of seconds used to specify an acceptable error range. Use this option when the OCSP responder clock and a client clock are not synchronized, which can cause a certificate status check to fail. This value must be a positive number. The default value is 300 seconds.

◆ verify
  Enables or disables verification of an OCSP response signature or the nonce values. Used for debugging purposes only. The default value is enabled.

◆ verify-cert
  Specifies that the system makes additional checks to see if the signer's certificate is authorized to provide the necessary status information. Use this option for testing purposes only. The default value is enabled.

◆ verify-other
  Specifies the name of the file used to search for an OCSP response signing certificate when the certificate has been omitted from the response. The default value is none.

◆ verify-sig
  Specifies that the system checks the signature on the OCSP response. Use this option for testing purposes only. The default value is enabled.

See also

create, delete, edit, glob, list, ltm auth profile, ltm auth ssl-ocsp, ltm virtual, modify, regex, show, tmsh
profile

Configures an authentication profile.

Module

ltm auth

Syntax

Configure the profile component within the ltm auth module using the following syntax.

Create/Modify

create profile [name]
modify profile [name]
  options:
    configuration [ [name] | none]
    cookie-key [string]
    cookie-name [string]
    credential-source [http-basic-auth]
    defaults-from [name]
    description [string]
    enabled [yes | no]
    idle-timeout [integer]
    rule [iRule name]
    edit auth [ [ [name] | [glob] | [regex] ] ... ]
      options:
        all-properties
        non-default-properties
    reset-stats auth
    reset-stats auth [ [ name ] | [ glob ] | [ regex ] ] ... ]

Display

list auth
list auth [ [ name ] | [ glob ] | [ regex ] ] ... ]
show running-config auth
show running-config auth [ [ name ] | [ glob ] | [ regex ] ] ... ]
  options:
    all-properties
    non-default-properties
    one-line
Partition

Show auth

```
show auth [ [ [name] | [glob] | [regex] ] ... ]
```

Options:

- (default | exa | gig | kil | meg | peta | raw | tera | yotta | zetta)
- field-fmt
- global

Delete

```
delete auth [name]
```

Notes

- You cannot delete default profiles.

Description

You can use the `profile` component to configure a custom authentication profile, or you can use the default profile that the BIG-IP Local Traffic Manager system provides for each type of authentication module.

An authentication profile requires one of the following configuration objects: `ltm auth kerberos-delegation`, `ltm auth ldap`, `ltm auth radius`, `ltm auth ssl-cc-ldap`, `ltm auth ssl-crldp`, `ltm auth ssl-oscp` or `ltm auth tacacs`. The type of profile specified by the `defaults-from` option must match the type of configuration object.

Examples

```
Creates a profile named `my_authentication_profile` for TACACS+ authentication:

create profile my_authentication_profile {
    configuration tacacs defaults-from tacacs credential-source http-basic-auth \
        enabled yes idle-timeout 30 rule _sys_auth_tacacs
}
```

Displays the properties of all of the `auth profile` components:

```
list profile
```

Options

You can use these options with the `auth` component:

- `configuration`
  - Specifies the name of an authentication configuration object. This option is required.
◆ cookie-key
   Specifies the key that the system uses to encrypt the session cookie assigned to each user using the cookie-name option. The default value is f5auth. This option applies only to KRB Delegate profiles.

◆ cookie-name
   Specifies a session cookie assigned to each user. F5 Networks recommends that each virtual server use a different cookie name. The system encrypts the cookie using the value of the cookie-key option. The default value is abc123. This option applies only to KRB Delegate profiles.

◆ credential-source
   Specifies the credential source.

◆ description
   User-defined description.

◆ defaults-from
   Specifies the name of the authentication profile from which you want your custom profile to inherit settings. This option is required.

◆ enabled
   Specifies whether the authentication profile is enabled. The default value is yes.

◆ glob
   Displays the items that match the glob expression. For a description of glob expression syntax, see the glob man page.

◆ idle-timeout
   Specifies the idle timeout for the authentication profile. The default value is 300 seconds.

◆ name
   Specifies a unique name for the component. This option is required for the commands create, delete, and modify.

◆ partition
   Displays the administrative partition in which the component resides.

◆ regex
   Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. For a description of regular expression syntax, see the regex man page.

◆ rule
   Specifies the name of the rule that corresponds to the authentication method you want to use.
See also

cREATE, DELETE, EDIT, GLOB, LTM AUTH CRLDP-SERVER, LTM AUTH KERBEROS-DELEGATION, LTM AUTH LDAP, LTM AUTH O CSP-RESPONDER, LTM AUTH RADIUS, LTM AUTH RADIUS-SERVER, LTM AUTH SSL-CC-LDAP, LTM AUTH SSL-CRLDP, LTM AUTH SSL-O CSP, LTM AUTH TACACS, LIST, LTM VIRTUAL, MODIFY, REGEX, RESET-STATS, SHOW, TMSSH
radius

Configures a RADIUS configuration object for implementing remote
RADIUS-based client authentication of BIG-IP system users.

Module

ltm auth

Syntax

Configure the radius component within the ltm auth module using the
following syntax.

Create/Modify

create radius [name]
modify radius [name]

options:
  accounting-bug [disabled | enabled]
  client-id [none | [string] ]
  debug [disabled | enabled]
  description [string]
  retries [integer]
  service-type [default | login | framed | callback-login | callback-framed | outbound |
             administrative | nas-prompt | authenticate-only | callback-nas-prompt | call-check |
             callback-administrative]
  servers [add | delete | replace-all-with] { [ [hostname ... ] | [ip address ... ] ] }
  servers [default | none]
edit radius [ [ [name] | [glob] | [regex] ] ... ]

options:
  all-properties
  non-default-properties

Display

list radius
list radius [ [ [name] | [glob] | [regex] ] ... ]
show running-config radius
show running-config radius [ [ [name] | [glob] | [regex] ] ... ]

options:
  all-properties
  non-default-properties
  one-line
  partition
Delete

delete radius [name]

Description

You use a RADIUS authentication module when your authentication data is stored on a remote RADIUS server. In this case, client credentials are based on basic HTTP authentication (that is, user name and password).

To implement a RADIUS authentication module and create a RADIUS configuration object

1. Use the radius-server component in the ltm auth module to configure a RADIUS server.
2. Use the radius component in the ltm auth module to create a RADIUS configuration object that references the RADIUS server you created in Step 1.
3. Use the profile component in the ltm auth module to create an authentication profile in which you specify the following options:
   a) For the configuration option, specify the RADIUS configuration object that you created in Step 2.
   b) For the defaults-from option, specify a parent profile (either the default RADIUS profile named radius or another custom profile that you created).

Examples

Creates a RADIUS configuration object named my_auth_radius:
create radius my_auth_radius servers add {10.10.10.1}

Deletes the RADIUS configuration object named my_auth_radius:
delete radius my_auth_radius

Options

You can use these options with the radius component:

- accounting-bug
  Enables or disables validation of the accounting response vector. This option is necessary only on older servers. The default value is disabled.

- client-id
  Sends a NAS-Identifier RADIUS attribute. If you do not specify a value for the client-id option, the system uses the pluggable authentication module (PAM) service type. You can disable this feature by specifying a blank client ID.
◆ **debug**
Enables or disables `syslog-ng` debugging information at `LOG DEBUG` level. F5 Networks does not recommend this option for normal use. The default value is **disabled**.

◆ **description**
User-defined description.

◆ **glob**
Displays the items that match the `glob` expression. For a description of `glob` expression syntax, see the `glob` man page.

◆ **name**
Specifies a unique name for the component. This option is required for the commands `create`, `delete`, and `modify`.

◆ **partition**
Displays the administrative partition within which the component resides.

◆ **regex**
Displays the items that match the regular expression. The regular expression must be preceded by an at sign (`[@regular expression]`) to indicate that the identifier is a regular expression. For a description of regular expression syntax, see the `regex` man page.

◆ **retries**
Specifies the number of authentication retries that the BIG-IP Local Traffic Manager system accepts before authentication fails. The default value is 3.

◆ **service-type**
Specifies the type of service used for the RADIUS server. The default is `default`, which behaves as `authenticate-only`.

◆ **servers**
Specifies the hostnames or IP addresses of the RADIUS servers that the BIG-IP Local Traffic Manager system uses to obtain authentication data. For more information about creating RADIUS server objects, see `radius-server`, on page 23-25.

---

**See also**

`create`, `delete`, `edit`, `glob`, `list`, `ltm auth profile`, `ltm auth radius-server`, `ltm virtual`, `modify`, `regex`, `show`, `tmsh`
radius-server

Configures a RADIUS server for implementing remote RADIUS-based client authentication.

Module

tlm auth

Syntax

Configure the radius-server component within the tlm auth module using the following syntax.

Create/Modify

create radius-server [name]
modify radius-server [name]
  options:
    description [string]
    port [ [name] | [number] ]
    secret [none | "string"]
    server [ [hostname] | [ip address] | none ]
    timeout [integer]
edit radius-server [ [ [name] | [glob] | [regex] ] ... ]
  options:
    all-properties
    non-default-properties

Display

list radius-server
list radius-server [ [ [name] | [glob] | [regex] ] ... ]
show running-config radius-server
show running-config radius-server [ [ [name] | [glob] | [regex] ] ... ]
  options:
    all-properties
    non-default-properties
    one-line
    partition

Delete

delete radius-server [name]
Description

You use a RADIUS authentication module when your authentication data is stored on a remote RADIUS server. In this case, client credentials are based on basic HTTP authentication (that is, user name and password).

To configure a RADIUS authentication module and create a RADIUS server

1. Use the `radius-server` component in the `ltm auth` module to configure a RADIUS server.

2. Use the `radius` component in the `ltm auth` module to create a RADIUS configuration object that references the RADIUS server you created in Step 1.

3. Use the `profile` component in the `ltm auth` module to create an authentication profile in which you specify the following two options:
   a) For the `configuration` option, you specify the `radius` component that you created in Step 2.
   b) For the `defaults-from` option, you specify a parent profile (either the default RADIUS profile named `radius` or another custom profile that you created).

Examples

Creates a RADIUS server named `my_radius_server`:

```
create radius-server bigip_auth_radius_server secret "This is the secret." server 10.1.1.1
```

Deletes the RADIUS server named `my_radius_server`:

```
delete radius-server my_radius_server
```

Options

You can use these options with the `radius-server` component:

- **description**
  User-defined description.

- **glob**
  Displays the items that match the `glob` expression. For a description of `glob` expression syntax, see the `glob` man page.

- **name**
  Specifies a unique name for the component. This option is required for the commands `create`, `delete`, and `modify`.

- **partition**
  Displays the administrative partition within which the component resides.
◆ **port**
  Specifies the port for RADIUS authentication traffic. The default value is 1812.

◆ **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. For a description of regular expression syntax, see the `regex` man page.

◆ **secret**
  Specifies the secret key the system uses to encrypt and decrypt packets sent or received from the server. This option is required.

◆ **server**
  Specifies the host name or IP address of the RADIUS server. This option is required.

◆ **timeout**
  Specifies the timeout value in seconds. The default value is 3 seconds.

### See also

create, delete, edit, glob, list, ltm auth profile, ltm auth radius, ltm virtual, modify, regex, show, tmsh
ssl-cc-ldap

Configures an SSL client certificate configuration object for remote SSL-based LDAP authorization for client traffic passing through the traffic management system.

Module

ltm auth

Syntax

Configure the ssl-cc-ldap component within the ltm auth module using the following syntax.

Create/Modify

create ssl-cc-ldap [name]
modify ssl-cc-ldap [name]

options:
admin-dn [ [name] | none]
admin-password [none | [password] ]
cache-size [integer]
cache-timeout [integer]
certmap-base [none | [search base] ]
certmap-key [ [name] | none)
certmap-user-serial [no | yes]
description [string]
group-base [none | [search base] ]
group-key [ [name] | none]
group-member-key [ [name] | none]
role-key [ [name] | none]
search-type [cert | certmap | user]
secure [no | yes]
servers [add | delete | replace-all-with] { [ip address ... ] }
servers none
user-base [none | [search base] ]
user-class [ [class] | none]
user-key [ [key] | none]
valid-groups [add | delete | replace-all-with] { [group ... ] }
valid-groups none
valid-roles [add | delete | replace-all-with] { [role ... ] }
valid-roles none
edit ssl-cc-ldap [ [name] | [glob] | [regex] ] ...

options:
  all-properties
  non-default-properties

Display

list ssl-cc-ldap
list ssl-cc-ldap [ [name] | [glob] | [regex] ] ...
show running-config ssl-cc-ldap
show running-config ssl-cc-ldap [ [name] | [glob] | [regex] ] ...

options:
  all-properties
  non-default-properties
  one-line
  partition

Delete

delete ssl-cc-ldap [name]

Description

You can use the ssl-cc-ldap component to configure SSL client certificate-based remote LDAP authorization for client traffic passing through the traffic management system.

To configure this type of authentication module and create a configuration object

1. Use the ssl-cc-ldap component in the ltm auth module to create an SSL client certificate LDAP configuration object.

2. Use the profile component in the ltm auth module to create an authentication profile in which you specify the following two options:
   a) For the configuration option, specify the configuration object that you created in Step 1.
   b) For the defaults-from option, specify a parent profile (either the default profile named ssl_cc_ldap or another custom profile that you created).
Options

You can use these options with the `ssl-cc-ldap` component:

- **admin-dn**
  Specifies the distinguished name of an account to which to bind, to perform searches. This search account is a Read-only account used to do searches. The `admin` account can also be used as the search account. If no admin DN is specified, then no bind is attempted.
  This option is required only when an LDAP database does not allow anonymous searches. The default value is `none`.

- **admin-password**
  Specifies the password for the `admin` account. See the `admin-dn` option. The default value is `none`.

- **cache-size**
  Specifies the maximum size, in bytes, allowed for the SSL session cache. Setting this option to 0 (zero) disallows SSL session caching. The default value is `20000` bytes (20KB).

- **cache-timeout**
  Specifies the number of usable lifetime seconds of negotiable SSL session IDs. When this time expires, a client must negotiate a new session. The default value is 300 seconds.

- **certmap-base**
  Specifies the search base for the subtree used by the `certmap` search method. A typical search base is: `ou=people,dc=company,dc=com`. The default value is `none`.

- **certmap-key**
  Specifies the name of the certificate map that the `certmap` search method uses. This name is found in the LDAP database. The default value is `none`.

- **certmap-user-serial**
  Specifies whether the system uses the client certificate's subject or serial number (in conjunction with the certificate's issuer) when trying to match an entry in the certificate map subtree.
  A value of `yes` uses the serial number. A value of `no` uses the subject. The default value is `no`.

- **description**
  User-defined description.

- **glob**
  Displays the items that match the `glob` expression. For a description of `glob` expression syntax, see the `glob` man page.

- **group-base**
  Specifies the search base for the subtree used by group searches. Use this option only when specifying the `valid-groups` option. The typical search base is similar to: `ou=groups,dc=company,dc=com`. The default value is `none`. 
◆ **group-key**  
Specifies the name of the attribute in the LDAP database that specifies the group name in the group subtree. An example of a typical key is `cn` (common name for the group). The default value is `none`.

◆ **group-member-key**  
Specifies the name of the attribute in the LDAP database that specifies members (DNs) of a group. A typical key is `member`. The default value is `none`.

◆ **name**  
Specifies a unique name for the component. This option is required for the commands `create`, `delete`, and `modify`.

◆ **partition**  
Displays the administrative partition within which the component resides.

◆ **regex**  
Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. For a description of regular expression syntax, see the `regex` man page.

◆ **role-key**  
Specifies the name of the attribute in the LDAP database that specifies a user's authorization roles. Use this option only when specifying the `valid-roles` option. A typical role key is `authorizationRole`. The default value is `none`.

◆ **search**  
Specifies the type of LDAP search that is performed based on the client's certificate. Possible values are:

- **cert**: Searches for the exact certificate.
- **certmap**: Searches for a user by matching the certificate issuer and the certificate serial number or certificate.
- **user**: Searches for a user based on the common name found in the certificate. This is the default value.

◆ **secure**  
Specifies whether the system attempts to use secure LDAP (LDAP over SSL). The alternative to using secure LDAP is to use insecure (clear text) LDAP. Secure LDAP is a consideration when the connection between the BIG-IP system and the LDAP server cannot be trusted. The default value is `no`.

◆ **servers**  
Specifies a list of LDAP servers you want to search. You must specify a server when you create an SSL client certificate configuration object.

◆ **user-base**  
Specifies the search base for the subtree used when you select for the `search` option either of the values `user` or `cert`. A typical search base is `ou=people,dc=company,dc=com`. You must specify a user base when you create an SSL client certificate configuration object. The default value is `none`. 
◆ **user-class**  
Specifies the object class in the LDAP database to which the user must belong to be authenticated. The default value is none.

◆ **user-key**  
Specifies the key that denotes a user ID in the LDAP database (for example, the common key for the user option is uid). You must specify a user key when you create an SSL client certificate configuration object.

◆ **valid-groups**  
Specifies a space-delimited list of the names of groups that the client must belong to be authorized (matches against the group key in the group subtree). The client needs to be a member of only one of the groups in the list. The default value is none.

◆ **valid-roles**  
Specifies a space-delimited list of the valid roles that clients must have to be authorized. The default value is none.

**See also**

create, delete, edit, glob, list, ltm auth profile, ltm virtual, modify, regex, show, tmsh
ssl-crldp

Configures a Secure Socket Layer (SSL) Certificate Revocation List Distribution Point (CRLDP) configuration object for implementing SSL CRLDP to manage certificate revocation.

Module

ltm auth

Syntax

Configure the ssl-crldp component within the ltm auth module using the following syntax.

Create/Modify

create ssl-crldp [name]
modify ssl-crldp [name]

options:
  cache-timeout [integer]
  connection-timeout [integer]
  description [string]
  servers [add | delete | replace-all-with] ( [ip address ... ] )
  servers [default | none]
  update-interval [integer]
  use-issuer [disabled | enabled]
edit ssl-crldp [ [ [name] | [glob] | [regex] ] ... ]

options:
  all-properties
  non-default-properties

Display

list ssl-crldp
list ssl-crldp [ [ [name] | [glob] | [regex] ] ... ]

show running-config ssl-crldp
show running-config ssl-crldp [ [ [name] | [glob] | [regex] ] ... ]

options:
  all-properties
  non-default-properties
  one-line
  partition
Chapter 23

Delete

```
delete ssl-crldp [name]
```

Description

CRLDP authentication is a mechanism for checking certificate revocation status for client connections passing through the system. This module is useful when your authentication data is stored on a remote CRLDP server.

**To implement a CRLDP authentication module and create an SSL CRLDP configuration object**

1. Use the `crldp-server` component in the `ltm auth` module to create a CRLDP server.
2. Use the `ssl-crldp` component in the `ltm auth` module to create a CRLDP configuration object.
3. Use the `profile` component in the `ltm auth` module to create an authentication profile in which you specify the following two options:
   a) For the `configuration` option, specify the CRLDP configuration object that you created in Step 2.
   b) For the `defaults-from` option, specify a parent profile (either the default profile named `ssl_crldp` or another custom profile that you created).

Examples

Creates an SSL CRLDP configuration object named `my_auth_ssl-crldp`:
```
create ssl-crldp my_auth_ssl-crldp
```

Deletes the SSL CRLDP configuration object named `my_auth_ssl-crldp`:
```
delete ssl-crldp my_auth_ssl-crldp
```

Options

You can use these options with the `ssl-crldp` component:

- **cache-timeout**
  Specifies the number of seconds that CRLs are cached. The default value is **86400** (24 hours).
- **connection-timeout**
  Specifies the number of seconds before the connection times out. The default value is **15**.
- **description**
  User-defined description.
◆ **glob**
   Displays the items that match the **glob** expression. For a description of **glob** expression syntax, see the **glob** man page.

◆ **name**
   Specifies a unique name for the component. This option is required for the commands **create**, **delete**, and **modify**.

◆ **partition**
   Displays the administrative partition within which the component resides.

◆ **regex**
   Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. For a description of regular expression syntax, see the **regex** man page.

◆ **servers**
   Specifies a host name or IP address for the secure CRLDP server. This option is required. The default value is **none**.

◆ **update-interval**
   Specifies an update interval for CRL distribution points that ensures that CRL status is checked at regular intervals, regardless of the CRL timeout value. This helps to prevent CRL information from becoming outdated before the BIG-IP system checks the status of a certificate. The default value is 0 (zero), which indicates an internal default value is active.

◆ **use-issuer**
   Specifies whether the system extracts the CRL distribution point from the client certificate. The default value is **disabled**.

See also

create, delete, edit, glob, list, ltm auth profile, ltm auth crldp-server, ltm virtual, modify, regex, show, tmsh
ssl-ocsp

Configures OCSP authentication for client traffic passing through the traffic management system.

Module

ltm auth

Syntax

Configure the ssl-ocsp component within the ltm auth module using the following syntax.

Create/Modify

create ssl-ocsp [name]
modify ssl-ocsp [name]
  options:
    description [string]
    responders [add | delete | replace-all-with] { [name]... }
  responders [default | none]
edit ssl-ocsp [ [ [name] | [glob] | [regex] ] ... ]
  options:
    all-properties
    non-default-properties

Display

list ssl-ocsp
list ssl-ocsp [ [ [name] | [glob] | [regex] ] ... ]
show running-config ssl-ocsp
show running-config ssl-ocsp [ [ [name] | [glob] | [regex] ] ... ]
  options:
    all-properties
    non-default-properties
    one-line
    partition

Delete

delete ssl-ocsp [name]
Description

Online Certificate Status Protocol (OCSP) is an industry-standard protocol that offers an alternative to a certificate revocation list when using public-key technology.

To implement an SSL OCSP authentication module and create an SSL OCSP configuration object

1. Use the `ocsp-responder` component in the `ltm auth` module to configure an OCSP responder object.
2. Use the `ssl-ocsp` component in the `ltm auth` module to configure an SSL OCSP configuration object to which you add the OCSP responder object that you created in Step 1.
3. Use the `profile` component in the `ltm auth` module to create an authentication profile in which you specify the following two options:
   a) For the `configuration` option, specify the SSL OCSP configuration object that you created in Step 2.
   b) For the `defaults-from` option, specify a parent profile (either the default OCSP Responder profile named `ssl_ocsp` or another custom profile that you created).

Examples

Creates an SSL OCSP configuration object named `my_auth_ssl-ocsp`:

```
create ssl-ocsp my_auth_ssl-ocsp
```

Deletes the SSL OCSP configuration object named `my_auth_ssl-ocsp`:

```
delete ssl-ocsp my_auth_ssl-ocsp
```
◆ **regex**
   Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. For a description of regular expression syntax, see the `regex` man page.

◆ **responders**
   Specifies a list of OCSP responders that you configured using the `ocsp-responder` component in the `ltm auth` module.

See also

`create`, `delete`, `edit`, `glob`, `list`, `ltm auth profile`, `ltm auth ocsp-responder`, `ltm virtual`, `modify`, `regex`, `tmsh`
**tacacs**

Configure a TACACS+ configuration object for implementing remote TACACS+-based client authentication.

**Module**

**ltm auth**

**Syntax**

Configure the **tacacs** component within the **ltm auth** module using the following syntax.

**Create/ Modify**

- `create tacacs [name]`
- `modify tacacs [name]`

**options:**
- `accounting [send-to-all-servers | send-to-first-server]`
- `authentication [use-all-servers | use-first-server]`
- `debug [disabled | enabled]`
- `description [string]`
- `encryption [disabled | enabled]`
- `protocol [none | [protocol] ]`
- `secret [ "[string]" ]`
- `servers [add | delete | replace-all-with] { [hostname ... ] | [ip address ... ] }`
- `service [ [name] | none]`
- `edit tacacs [ [ [name] | [glob] | [regex] ] ... ]`

**options:**
- `all-properties`
- `non-default-properties`

**Display**

- `list tacacs`
- `list tacacs [ [name] | [glob] | [regex] ] ... ]`
- `show running-config tacacs`
- `show running-config tacacs [ [name] | [glob] | [regex] ] ... ]`

**options:**
- `all-properties`
- `non-default-properties`
- `one-line`
- `partition`
Delete

```
delte tacacs [name]
```

Description

Using a TACACS+ configuration object and profile, you can implement the TACACS+ authentication module as the mechanism for authenticating client connections passing through the BIG-IP Local Traffic Manager system. You use this module when your authentication data is stored on a remote TACACS+ server. In this case, client credentials are based on basic HTTP authentication (that is, user name and password).

To implement a TACACS+ authentication module and create a TACACS+ configuration object

1. Use the `tacacs` component in the `ltm auth` module to configure a TACACS+ configuration object.
2. Use the `profile` component in the `ltm auth` module to create an authentication profile in which you specify the following two options:
   a) For the `configuration` option, specify the TACACS+ configuration object that you created in Step 1.
   b) For the `defaults-from` option, specify a parent profile (either the default TACACS+ profile named `tacacs` or another custom profile that you created).

Examples

Enables encryption for TACACS+ packets:

```
create tacacs my_tacacs_auth secret "This is the secret" servers add {my_tacacs_server} encryption enabled
```

Provides the ability to send accounting start and stop packets to all servers:

```
create tacacs my_tacacs_auth secret "This is the secret" servers add { my_tacacs_server1 my_tacacs_server2 } accounting send-to-all-servers
```

Options

You can use these options with the `ltm auth tacacs` component:

- **accounting**
  If multiple TACACS+ servers are defined and pluggable authentication module (PAM) session accounting is available, specifies where the system sends accounting start and stop packets. Possible values are:
  - **send-to-all-servers**
    Sends to all servers.
- **send-to-first-server**
  Sends to the first available server.

- **authentication**
  Specifies when to use the secret key supplied for the `secret` option. This option is required.
  The options are:
  - **use-all-servers**
    Use the secret key with all servers.
  - **use-first-server**
    Use the secret key with the first available server.

- **debug**
  Enables syslog-ng debugging information at LOG DEBUG level. F5 Networks does not recommend this option for normal use. The default value is `disabled`.

- **description**
  User-defined description.

- **encryption**
  Enables or disables encryption of TACACS+ packets. Recommended for normal use. The default value is `enabled`.

- **first-hit**
  Confirms the secret key supplied for the `secret` option. This option is required. The default value is `disabled`.

- **glob**
  Displays the items that match the `glob` expression. For a description of `glob` expression syntax, see the `glob` man page.

- **name**
  Specifies a unique name for the component. This option is required for the commands `create`, `delete`, and `modify`.

- **partition**
  Displays the administrative partition within which the component resides.

- **protocol**
  Specifies the protocol associated with the value specified in the `service` option, which is a subset of the associated service being used for client authorization or system accounting.

- **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. For a description of regular expression syntax, see the `regex` man page.

- **secret**
  Sets the secret key used to encrypt and decrypt packets sent or received from the server. This option is required.

- **servers**
  Specifies a host name or IP address for the TACACS+ server. This option is required.
• **service**
  Specifies the name of the service that the user is requesting to be authenticated to use. Identifying the service enables the TACACS+ server to behave differently for different types of authentication requests. This option is required.

**See also**

create, delete, edit, glob, list, ltm auth profile, ltm virtual, modify, regex, show, tmsh
Introducing the LTM classification module

Alphabetical list of components
Introducing the ltm classification module

You can use the tmsh components that reside within the ltm classification module to configure classification signatures, keys, and so on. For more information about the tmsh hierarchical structure, see Chapter 2, Understanding and Using the Traffic Management Shell.

Alphabetical list of components

The remainder of this chapter lists the tmsh components that are available in the ltm classification module.
category

Configures a custom classification category.

Module

ltm classification

Syntax

Configure the category component within the ltm classification module using the syntax shown in the following sections.

Create/Modify

create category [object identifier]

Display

list category
list category [all | object identifier]
show running-config category
show running-config category [all | object identifier]
options:
  all-properties
  non-default-properties

Delete

delete category [object identifier]

Description

You can use the category component to create, delete, and display a classification category profile.
Examples

Creates a new category named **my_cat**:

```bash
create category my_cat
```

Displays all created categories:

```bash
list category
```

Deletes the category named **my_cat**:

```bash
delete category my_cat
```

Options

You can use this option with the **category** component:

- **object identifier**
  
  Specifies a unique identifier for the category. This option is required for the **create category** and **delete category** commands.

See also

create, delete, list, ltm classification, show, tmsh
http-signature

Configures a custom classification HTTP signature.

Module

ltm classification

Syntax

Configure the http-signature component within the ltm classification module using the following syntax.

Create/Modify

create http-signature [object identifier] application [app_name] category [cat_name]
modify http-signature [object identifier] application [app_name] category [cat_name]
options:
   req-key-values [ [add | del | modify | replace-all-with] { [ Content-Type {value [value_name]} | Host {value [value_name]} | Referer {value [value_name]} | User-Agent {value [value_name]} | host {value [value_name]} | hostprefix {value [value_name]} | uri {value [value_name]} | custom_key1 {value [value_name]} | custom_key2 {value [value_name]} ] | none] }
   resp-key-values [ [add | del | modify | replace-all-with] { [ Content-Type {value [value_name]} | customem_key1 {value [value_name]} | customem_key2 {value [value_name]} ] | none] }
edit http-signature [object identifier | all]
options:
   all-properties
   non-default-properties

Display

list http-signature
list http-signature [all | object identifier]
show running-config http-signature
show running-config http-signature [all | object identifier]  
options:  
  all-properties  
  non-default-properties  
  one-line

Description

You can use the `http-signature` component to create, delete, and display a classification HTTP signature profile that combines categories and key values of interest. It matches the HTTP traffic with key values defined in the signature. If there is a match, the corresponding `application-name` will be used to identify it.

Examples

Creates an HTTP signature named `testSig` of application type `gnutella` and category `p2p` and adds an HTTP Request key of `User-Agent` and a value of `gnutella`:

```
<create http-signature testSig application gnutella category p2p req-key-values add
   {User-Agent {value gnutella}}
```

Displays all HTTP signatures:

```
list http-signature
```

Displays the HTTP signature uniquely identified by object identifier:

```
list http-signature [object identifier]
```

Deletes an HTTP signature named `testSig`:

```
delete http-signature testSig
```

Deletes all HTTP signatures:

```
delete http-signature all
```

Options

You can use these options with the `http-signature` component:

- **application**  
  Allows the user to specify an application name. This field can be reused by other signatures as well.

- **category**  
  Allows the user to specify a category with the HTTP signature. The specified category could be one of the predefined ones (for example: `All, Encrypted, Web, Audio, P2P, video`) or a user-specified category that was previously defined.
◆ **object identifier**
Specifies a unique identifier for the HTTP signature. This option is required for the create category and delete category commands.

◆ **req-key-value**
Allows the user to create one or more HTTP Request Key/Value pairs. Custom keys must first be created by using create classification key.

◆ **resp-key-values**
Allows the user to create one or more HTTP Response Key/Value pairs. Custom keys must first be created by using create classification key.

*Note: Host, hostprefix, User-Agent, and uri cannot be added to resp-key-values.*

See also

create, delete, edit, list, ltm classification, modify, regex, show, tmsh
key

Configures a custom classification key.

Module

ltm classification

Syntax

Configure the key within the ltm classification module using the syntax shown in the following sections.

Create

create key [object identifier]
  options:
    priority [integer]

Display

list key
list key [all | object identifier]
show running-config key
show running-config key [all | object identifier]
  options:
    all-properties
    non-default-properties
    one-line

Delete

delete key [object identifier]

Description

You can use the key component to create, delete, and display a classification key profile. Host, hostprefix, uri, User-Agent, Content-Type, and Content-Length are system-defined keys and cannot be deleted.

Priority specifies the order in which keys will be given preference. Priority can be any integer starting from 6 (six). Priority numbers 0 (zero) through 5 (five) are system-defined cannot be modified.

If no priority is specified, the next available priority number will be assigned.
For example, if there are two keys K2 and K1 with priority set as 9 (nine) and 10 (ten), there are two signatures S1 {K1: V1} and S2 {K2: V2}, and if HTTP traffic contains the pattern K1:V1 and K2:V2, then the S2 Signature will be matched for this traffic.

Priority is used to resolve conflicts among signatures. If the user does not specify a priority number, the next available priority number will be assigned automatically.

Although you can modify keys, there is no validation check to ensure that all keys have unique priorities. Keys need to have unique priority numbers.
You can create up to a maximum of 225 custom-defined keys.

Examples

Creates a new custom classification key named my_key:

```
create key my_key
```

Creates a new custom classification key named my_key with priority 10:

```
create key my_key priority 10
```

Changes the custom classification key named my_key from priority 10 to priority 6:

```
modify key my_key priority 6
```

Displays all the classification keys:

```
list key
```

Deletes a previously configured classification key named my_key:

```
delete key my_key
```

Options

You can use this option with the key component:

◆ object identifier
  Specifies a unique identifier for the key. This option is required for the create category and delete category commands.

See also

list, ltm classification, show, tmsh
signature-update-schedule

Configures scheduling for classification signature updates.

Module

ltm classification

Syntax

Configure the category within the ltm classification module using the syntax shown in the following sections.

Create/Modify

create signature-update-schedule [name]
modify signature-update-schedule [name]

options:

 [auto-update-enabled | auto-update-disabled]
auto-update-interval [daily | weekly | monthly]

Display

list signature-update-schedule
show running-config signature-update-schedule

options:

all-properties

Description

You can use the signature-update-schedule component to configure scheduling for classification signature updates.

Examples

Displays classification signature update scheduling configuration:

list signature-update-schedule

Updates the scheduler for classification signature updates to run once a day:

modify signature-update-schedule sched auto-update-enabled auto-update-interval daily

Disables the scheduler and allows signatures to update using the browser-based Configuration utility only:

modify signature-update-schedule sched auto-update-disabled
Options

You can use these options with the `signature-update-schedule` component:

- **auto-update-disabled**
  Specifies that the updates scheduler is disabled. The user can update the classification signatures using the browser-based BIG-IP® Configuration utility.

- **auto-update-enabled**
  Specifies that the updates scheduler is enabled.

- **auto-update-interval**
  Specifies the auto-update frequency for classification signatures. This attribute will only apply in case auto update is enabled. The default value is `daily`.

See also

list, modify, tmsh
update-signatures

Runs automatic update for classification signatures.

Module

ltm classification

Syntax

Run the update-signatures component within the ltm classification module using the syntax shown in the following sections.

Run

run update-signatures

Description

You can use the update-signatures component to update the classification signatures. Only admins can run this command.

See also

ltm classification signature-update-schedule, run, tmsh
ltm data-group Module Components

- Introducing the ltm data-group module
- Alphabetical list of components
Introducing the ltm data-group module

You can use the tmsh components that reside within the ltm data-group module to create a data-group that contains records that can be used from within an iRule. For more information about the tmsh hierarchical structure, see Chapter 2, Understanding and Using the Traffic Management Shell.

Alphabetical list of components

The remainder of this chapter lists the tmsh components that are available in the ltm data-group module.
external

Configures an external class.

Module

ltm data-group

Syntax

Configure the external data-group within the ltm data-group module using the syntax shown in the following sections.

Create/Modify

create external [name]
modify external [name]
  options:
   description [string]
   external-file-name [file name] | none
   separator [string]
   source-path [URL]
   type [integer | ip | string]
edit external [name] | [glob] | [regex] ... 
  options:
   all-properties
   non-default-properties

Display

list external
list external [name] | [glob] | [regex] ... 
show running-config external
show running-config external [name] | [glob] | [regex] ... 
  options:
   all-properties
   non-default-properties
   one-line
   partition
Description

Data groups are lists of data that you define and use with iRules® operators. External data group records are stored in external files that you manage through the **sys file data-group** component. Note that external data groups can be very large, which is one reason why the groups are saved to external files. For example, a phone company can store a list of thousands of phone numbers in an external data group.

You should consider using an internal data group when the number of records is expected to be small.

An external data group acquires its type from the associated data-group file, which can be a list of IP addresses, strings, or integers.

External data groups are lists that specify:

- A data-group file where records are stored
- A description of the class

There are two ways to configure the external data-group object:

- Create external data-group object, and then specify the **source-path** and type of the external-file. In one step, the external-file will be created within the **sys file data-group** module and external data-group within the **ltm data-group** module.

- Create an external-file within the **sys file data-group** module, and then create external data-group within the **ltm data-group** module. See **help sys file data-group** for information on creating the data-group file.

Examples

Creates an external data group named **ext-dg1**, with the given description. The records for the data group are loaded from the data-group file **string.dat** previously created in the **sys file data-group** component.

```bash
create external ext-dg1 external-file-name string.dat description "created for rule xyz"
```

Downloads the data-group file from the given URL into file-store and creates a data-group file named **ext_dg1** within the **sys file data-group** module. Creates an external data group named **ext-dg1**, with the given description. The records for the data group are loaded from the data-group file **ext_dg1**.

```bash
create external ext-dg1 description "created for rule xyz" source-path
    http://file-server/data-groups/ip.class type ip
```

Specifies the location of the file on the local disk (use this when the file has already been created on the local disk). Creates a data-group file named **ext_dg2** within the **sys file data-group** module. Creates an external data group named **ext-dg2**. The records for the data group are loaded from the data-group file **ext_dg2**.

```bash
create external ext-dg2 source-path file:/shared/save/Test.dat type string
```
Chapter 25

Downloads the file from the given URL into file_store and updates the source-path of data-group file referenced by external data group ext_dg2.

Modifies the description of external data group ext_dg2:

```plaintext
modify external ext-dg2 description "created for rule abc" source-path file:/shared/save/Test2.dat
```

Options

You can use these options with the external component:

- **description**
  User-defined description.

- **external-file-name**
  Specifies the data-group file where the records are stored.
  Note: Only source-path or external-file-name options can be specified for external data-group configuration item.

- **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. See help regex for a description of regular expression syntax.

- **separator**
  Specifies a separator to use when defining the data group. The default value is `:=`.

- **source-path [URL]**
  This optional attribute takes a URL, for example:
  ```plaintext
  source-path http://file-server/data-groups/AUL_1.cls
  source-path https://file-server/data-groups/CNN.x
  source-path ftp://username:password@server/data-groups/latest.class
  source-path file:/shared/save/Test.dat
  ```
  Note: Only source-path or external-file-name options can be specified for external data-group configuration item.

- **type**
  Specifies the kind of data in the group. This option is acquired from the data group file. If the external data group is created with external-file that was previously created within the sys file data-group module, then type option cannot be modified. If the external data group is created with source-path option, then type should be specified. Possible values for type are:
  - integer
  - ip
  - string
See also

create, delete, edit, glob, list, modify, regex, tmsh
internal

Configures an internal class.

Module

ltm data-group

Syntax

Configure the internal component within the ltm data-group module using the following syntax.

Create/Modify

create internal [name]
options:
  description [string]
  records [add | delete | modify | replace-all-with] {
  [record key] {
  data [value]
  }
  }
  records none
  type [integer | ip | [string]]
modify internal [name]
options:
  description [string]
  records [add | delete | modify | replace-all-with] {
  [record key] {
  data [value]
  }
  }
  records none
  edit internal [ [ [name] | [glob] | [regex] ] ... ]
options:
  all-properties
  non-default-properties

Display

list internal
list internal [ [ [name] | [glob] | [regex] ] ... ]
show running-config internal
show running-config internal [ [ name ] | [ glob ] | [ regex ] ] ...

options:
   all-properties
   non-default-properties
   one-line
   partition

Description

Data groups are lists of data that you define and use with iRules® operators. Consider using an external data group if the number of records is expected to be large.

The BIG-IP® system includes the following predefined lists that you can use:
   • aol
   • default_accept_language
   • images
   • private_net

These lists are located in the file /config/profile_base.conf. When you run the command load, the system loads these lists; however, unless you have modified the lists, the system does not save the lists to the bigip.conf file.

The internal data groups are stored in the bigip.conf file.

Internal data groups can be one of three types:
   • A list of IP addresses
   • A list of strings
   • A list of integers

Strings must be surrounded by quotation marks. Numbers can be either positive or negative. These groups define the type of data in the class, which can be IP addresses, strings, or integers

Examples

Creates an internal data group named MyDG that contains a single IP address:
   create internal MyDG records add { 10.0.0.0 } type ip

Creates an internal data group named DG2 that contains a list of three network addresses: 192.1.1.0/24, 192.2.1.1/24, and 192.3.1.24:
   create internal DG2 records add { 192.1.1.255 192.2.1.255 192.3.1.255 } type ip

Creates an internal data group named MyDG that contains a single name/value pair:
   create internal MyDG records add { my_key { data my_value } } type string
Options

You can use these options with the internal component:

- **description**
  User-defined description.

- **records**
  Configures the data in the group.

- **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. See help regex for a description of regular expression syntax.

- **type**
  Specifies the kind of data in the group. The default value is **ip**. This option is required by the command **create**.

See also

- **create**, **delete**, **edit**, **glob**, **list**, **modify**, **regex**, **tmsh**
itm dns cache Module Components

• Introducing the itm dns cache module
• Alphabetical list of components
Introducing the ltm dns cache module

You can use the tmsh components that reside within the ltm dns cache module to configure DNS caches for Local Traffic Manager™. For more information about the tmsh hierarchical structure, see Chapter 2, Understanding and Using the Traffic Management Shell.

Alphabetical list of components

The remainder of this chapter lists the tmsh components that are available in the ltm dns cache module.
global-settings

Configures the global settings of all DNS caches on the BIG-IP® system.

Module

ltm dns cache

Syntax

Configure the global-settings component within the ltm dns cache module using the following syntax.

Create/Modify

modify global-settings [name]
   options:
       cache-maximum-ttl [integer]
       cache-minimum-ttl [integer]
       resolver-edns-buffer-size [integer]
edit global-settings [ [ [name] | [glob] | [regex] ] ... ]
   options:
       all-properties
       non-default-properties

Display

list global-settings
list global-settings [ [ [name] | [glob] | [regex] ] ... ]
   options:
       all-properties
       non-default-properties
       one-line

Description

You can use the global-settings component to configure and view information about the global settings of all DNS caches.
Examples

Displays the global settings for the DNS caches on the BIG-IP system:

```
list global-settings all-properties
```

Options

You can use the following options with the `global-settings` component:

- **cache-maximum-ttl**
  Specifies the number of seconds after which you want the BIG-IP system to re-query for resource records. You can re-query sooner than the owner of the records intended.

- **cache-minimum-ttl**
  Specifies the minimum number of seconds you want the BIG-IP system to cache DNS resource records. You can cache resource records longer than the owner of the records intended.

- **glob**
  Displays the items that match the `glob` expression. See `help glob` for a description of `glob` expression syntax.

- **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (`@[regular expression]`) to indicate that the identifier is a regular expression. See `help regex` for a description of regular expression syntax.

- **resolver-edns-buffer-size**
  Specifies the number of bytes you want the BIG-IP system to advertise as the EDNS buffer size in UDP queries.

See also

```
create, edit, glob, list, modify, regex, tmsh
```
resolver

Configures a DNS cache with a resolver on the BIG-IP system.

Module

ltm dns cache

Syntax

Configure the resolver component within the ltm dns cache module using the following syntax.

Create/Modify

```
create resolver [name]
modify cache [name]
    options:
        answer-default-zones [yes | no]
        max-concurrent-tcp [integer]
        max-concurrent-udp [integer]
        msg-cache-size [integer]
        nameserver-cache-count [integer]
        root-hints {
            ( [IP address] ... )
        }
        route-domain [name]
        rrrset-cache-size [integer]
        unwanted-query-reply-threshold [integer]
        use-ipv4 [yes | no]
        use-ipv6 [yes | no]
        use-tcp [yes | no]
        use-udp [yes | no]
```

Display

```
list resolver
list resolver [ [name] | [glob] | [regex] ] ...
    options:
        all-properties
        non-default-properties
        one-line
    show resolver [name]
```
### Delete

```bash
delete resolver [name]
```

### Description

You can use the `resolver` component to configure and view information about a recursive-resolving DNS cache. A resolver cache performs recursive resolution to fill its cache.

**Important**

When sizing caches, consider the total amount of memory available and how you wish to allocate memory for DNS caching. Note that cache sizing values are per-TMM process; therefore, a platform with eight TMMs consumes the amount of memory set for the resource record set cache times eight.

### Examples

Displays the properties of the recursive-resolving DNS cache `myCache`:

```bash
list resolver myCache
```

### Options

You can use the following options with the `resolver` component:

- **answer-default-zones**
  Specifies whether the resolver cache answers queries for default zones: `localhost`, `reverse 127.0.0.1` and `::1`, and `AS112` zones. The default value is `no`.

- **glob**
  Displays the items that match the `glob` expression. See `help glob` for a description of `glob` expression syntax.

- **max-concurrent-tcp**
  Specifies the maximum number of concurrent TCP flows used by the resolver. The default value is `20`.

- **max-concurrent-udp**
  Specifies the maximum number of concurrent UDP flows used by the resolver. The default value is `8192`.

- **msg-cache-size**
  Specifies the maximum size in bytes of the DNS message cache. The default value is `1048576`.

  The BIG-IP system caches the messages in a DNS response in the message cache. After the maximum size of the cache is reached, when new or refreshed content is added to the cache, the expired and older content is removed from the cache. A higher maximum size allows more
DNS responses to be cached and increases the cache hit percentage. A lower maximum size forces earlier eviction of cached content, but can lower the cache hit percentage.

- **name**
  Specifies a unique name for the component. This option is required for the commands `create`, `delete`, and `modify`.

- **nameserver-cache-count**
  Specifies the maximum number of DNS nameservers for which the BIG-IP system caches connection and capability data. The default value is **16536** entries.

- **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. See `help regex` for a description of regular expression syntax.

- **root-hints**
  Specifies the IP addresses of DNS servers that the BIG-IP system considers authoritative for the DNS root nameservers.

  **Important:** By default, the BIG-IP system uses the DNS root nameservers published by InterNIC.

  **Important:** When you add DNS root nameservers, the BIG-IP system no longer uses the default nameservers published by InterNIC, but instead uses the nameservers you add as authoritative for the DNS root nameservers.

- **route-domain**
  Specifies the route domain the resolver uses for outbound traffic. The default value is the default route domain.

- **rrset-cache-size**
  Specifies the maximum size in bytes of the resource records set cache. The default value is **10485760**.

  The BIG-IP system caches the supporting records in a DNS response in the resource record cache. After the maximum size of the cache is reached, when new or refreshed content is added to the cache, the expired and older content is removed from the cache. A higher maximum size allows more DNS responses to be cached and increases the cache hit percentage. A lower maximum size forces earlier eviction of cached content, but can lower the cache hit percentage.

- **unwanted-query-reply-threshold**
  The system always rejects unsolicited replies. The default value of **0** (off) indicates the system does not generate SNMP traps or log messages when rejecting unsolicited replies.

  Change the default value, if you are using the BIG-IP system to monitor for unsolicited replies using SNMP. This alerts you to a potential security attack, such as cache poisoning or DOS. For example, if you specify 1,000,000 unsolicited replies, each time the system receives 1,000,000 unsolicited replies, it generates and SNMP trap and log message.
◆ **use-ipv4**
   When enabled, the resolver sends DNS queries to IPv4 addresses.

◆ **use-ipv6**
   When enabled, the resolver sends DNS queries to IPv6 addresses.

◆ **use-tcp**
   When enabled, the resolver can send queries over the TCP protocol.

◆ **use-udp**
   When enabled, the resolver can send queries over the UDP protocol.

**See also**

create, delete, edit, glob, list, ltm dns cache transparent, ltm dns cache validating-resolver, modify, regex, tmsh
transparent

Configures a DNS cache without a resolver on the BIG-IP system.

Module

ltm dns cache

Syntax

Configure the transparent component within the ltm dns cache module using the following syntax.

Create/Modify

create transparent [name]
modify cache [name]
  options:
    answer-default-zones [yes | no]
    dnssec-on-miss [yes | no]
    msg-cache-size [integer]
    rrset-cache-size [integer]

Display

list transparent
list transparent [ [ [name] | [glob] | [regex] ] ... ]
  options:
    all-properties
    non-default-properties
    one-line
    show transparent [name]

Delete

delete transparent [name]
Description

You can use the `transparent` component to configure and view information about a transparent DNS cache. A transparent cache does not perform recursive resolution, but instead relies on another DNS resource for this functionality.

**Important**

*When sizing caches, consider the total amount of memory available and how you wish to allocate memory for DNS caching. Note that cache sizing values are per-TMM process; therefore, a platform with eight TMMs consumes the amount of memory set for the resource record set cache times eight.*

Examples

Displays the properties of the transparent DNS cache `myCache`:

```
list transparent myCache
```

Options

You can use these options with the `transparent` component:

- **answer-default-zones**
  Specifies whether the resolver cache answers queries for default zones: `localhost`, `reverse 127.0.0.1`, `::1`, and `AS112` zones. The default value is `no`.

- **dnssec-on-miss**
  Specifies whether, on a cache miss, the BIG-IP system forwards queries after adding the DNSSEC OK bit. The default value is `yes`.

- **glob**
  Displays the items that match the `glob` expression. See `help glob` for a description of `glob` expression syntax.

- **msg-cache-size**
  Specifies the maximum size in bytes of the DNS message cache. The default value is `1048576`.

  The BIG-IP system caches the messages in a DNS response in the message cache. After the maximum size of the cache is reached, when new or refreshed content is added to the cache, the expired and older content is removed from the cache. A higher maximum size allows more DNS responses to be cached and increases the cache hit percentage. A lower maximum size forces earlier eviction of cached content, but can lower the cache hit percentage.

- **name**
  Specifies a unique name for the component. This option is required for the commands `create`, `delete`, and `modify`. 
◆ **regex**
Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. See `help regex` for a description of regular expression syntax.

◆ **rrset-cache-size**
Specifies the maximum size in bytes of the resource records set cache. The default value is **10485760**.

The BIG-IP system caches the supporting records in a DNS response in the resource record cache. After the maximum size of the cache is reached, when new or refreshed content is added to the cache, the expired and older content is removed from the cache. A higher maximum size allows more DNS responses to be cached and increases the cache hit percentage. A lower maximum size forces earlier eviction of cached content, but can lower the cache hit percentage.

### See also

create, delete, edit, glob, list, ltm dns cache resolver, ltm dns cache validating-resolver, modify, regex, tmsh
validating-resolver

Configures a DNS cache with a resolver and validator on the BIG-IP system.

Module

ltm dns cache

Syntax

Configure the validating-resolver component within the ltm dns cache module using the syntax in the following sections.

Create/Modify

create validating-resolver [name]
modify cache [name]

options:
  answer-default-zones [yes | no]
  dlv-anchors {
    { [DNSKEY or DS RR string] ... }
  }
  ignore-cd [yes | no]
  key-cache-size [integer]
  max-concurrent-udp [integer]
  max-concurrent-tcp [integer]
  msg-cache-size [integer]
  nameserver-cache-count [integer]
  prefetch-key [yes | no]
  root-hints {
    { [IP address] ... }
  }
  route-domain [name]
  rrset-cache-size [integer]
  trust-anchors {
    { [NDSKEY or DS RR string] ... }
  }
  unwanted-query-reply-threshold [integer]
  use-ipv4 [yes | no]
  use-ipv6 [yes | no]
  use-tcp [yes | no]
  use-udp [yes | no]
Display

list validating-resolver
list validating-resolver [ [ [name] | [glob] | [regex] ] ... ]
  options:
    all-properties
    non-default-properties
    pub-text
  show validating-resolver

Delete

delete validating-resolver [name]

Description

You can use the validating-resolver component to configure and view information about a validating recursive-resolving DNS cache. A resolving and validating cache performs recursive resolution to fill its cache and uses DNSSEC to ensure the integrity of the data.

Important

When sizing caches, consider the total amount of memory available and how you wish to allocate memory for DNS caching. Note that cache sizing values are per-TMM process; therefore, a platform with eight TMMs consumes the amount of memory set for the resource record set cache times eight.

Examples

Displays the properties of the validating recursive-resolving DNS cache myCache:

list validating-resolver myCache

Options

You can use the following options with the validating-resolver component:

- answer-default-zones
  Specifies whether the validating resolver cache answers queries for default zones: localhost, reverse 127.0.0.1 and ::1, and AS112 zones. The default value is no.

- dlv-anchors
  Specifies the DNSKEY or DS resource records the BIG-IP system uses to establish DNSSEC trust with a DLV registry. The resource records must be specified in string format, for example, dig or drill format. The default value is none.
- **glob**
  Displays the items that match the `glob` expression. See `help glob` for a description of `glob` expression syntax.

- **ignore-cd**
  Specifies, when enabled, the system ignores the **Checking Disabled** setting on client queries, performs validation, and returns only secure answers. The default value is `no`.

- **key-cache-size**
  Specifies the maximum size in bytes of the DNSKEY cache. The default value is `1048576`.

- **max-concurrent-tcp**
  Specifies the maximum number of concurrent TCP flows used by the resolver. The default value is `20`.

- **max-concurrent-udp**
  Specifies the maximum number of concurrent UDP flows used by the resolver. The default value is `8192`.

- **msg-cache-size**
  Specifies the maximum size in bytes of the DNS message cache. The default value is `1048576`.

  The BIG-IP system caches the messages in a DNS response in the message cache. After the maximum size of the cache is reached, when new or refreshed content is added to the cache, the expired and older content is removed from the cache. A higher maximum size allows more DNS responses to be cached and increases the cache hit percentage. A lower maximum size forces earlier eviction of cached content, but can lower the cache hit percentage.

- **name**
  Specifies a unique name for the component. This option is required for the commands `create`, `delete`, and `modify`.

- **nameserver-cache-count**
  Specifies the maximum number of DNS nameservers for which the BIG-IP system caches connection and capability data. The default value is `16536` entries.

- **prefetch-key**
  Specifies, when enabled, the validating resolver fetches the DNSKEY early in the validation process. Disable this setting, when you want to reduce resolver traffic, but understand that a client might have to wait for the validating resolver to perform a key lookup. The default value is `yes`.

- **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (`@[regular expression]`) to indicate that the identifier is a regular expression. See `help regex` for a description of regular expression syntax.

- **root-hints**
  Specifies the IP addresses of DNS servers that the BIG-IP system considers authoritative for the DNS root nameservers.
Important: By default, the BIG-IP system uses the DNS root nameservers published by InterNIC.

Important: When you add DNS root nameservers, the BIG-IP system no longer uses the default nameservers published by InterNIC, but uses the nameservers you add as authoritative for the DNS root nameservers.

- route-domain
  Specifies the route domain the resolver uses for outbound traffic. The default value is the default route domain.

- rrset-cache-size
  Specifies the maximum size in bytes of the resource records set cache. The default value is 10485760.

  The BIG-IP system caches the supporting records in a DNS response in the resource record cache. After the maximum size of the cache is reached, when new or refreshed content is added to the cache, the expired and older content is removed from the cache. A higher maximum size allows more DNS responses to be cached and increases the cache hit percentage. A lower maximum size forces earlier eviction of cached content, but can lower the cache hit percentage.

- trust-anchors
  Specifies the DNSKEY or DS resource records the BIG-IP system uses to establish DNSSEC trust with a specific DNS zone. The resource records must be specified in string format, for example, dig or drill format. The default value is none.

- unwanted-query-reply-threshold
  The system always rejects unsolicited replies. The default value of 0 (off) indicates the system does not generate SNMP traps or log messages when rejecting unsolicited replies.

  Change the default value, if you are using the BIG-IP system to monitor for unsolicited replies using SNMP. This alerts you to a potential security attack, such as cache poisoning or DOS. For example, if you specify 1,000,000 unsolicited replies, each time the system receives 1,000,000 unsolicited replies, it generates and SNMP trap and log message.

- use-ipv4
  When enabled, the resolver sends DNS queries to IPv4 addresses.

- use-ipv6
  When enabled, the resolver sends DNS queries to IPv6 addresses.

- use-tcp
  When enabled, the resolver can send queries over the TCP protocol.

- use-udp
  When enabled, the resolver can send queries over the UDP protocol.

See also

create, delete, edit, glob, list, ltm dns cache transparent, ltm dns cache resolver, modify, regex, tms
Ltm dns cache records Module Components

- Introducing the Ltm dns cache records module
- Alphabetical list of components
Introducing the ltm dns cache records module

You can use the `tmsh` components that reside within the **ltm dns cache records** module to configure DNS cache records for Local Traffic Manager™. For more information about the `tmsh` hierarchical structure, see Chapter 2, *Understanding and Using the Traffic Management Shell*.

Alphabetical list of components

The remainder of this chapter lists the `tmsh` components that are available in the **ltm dns cache records** module.
key

Manages the DNSKEY records in the DNS caches on the BIG-IP® system.

Module

ltm dns cache records

Syntax

Configure the key component within the ltm dns cache records module using the following syntax.

Display

show key cache [cache name]
options:
  group [integer]
  owner [domain name]
  slot [integer]
  tmm [integer]

Delete

delete key cache [cache name]
options:
  group [integer]
  owner [domain name]
  slot [integer]

Description

You can use the key component within the ltm dns cache records module to display and delete DNSKEY records.

Examples

Displays the DNSKEY records in the cache named resolver_cache:
show key cache resolver_cache

Deletes the DNSKEY records from the cache named v_resolver_cache:
delete key cache v_resolver_cache
## Options

You can use the following options with the `key` component:

- **cache name**
  Specifies a DNS cache from which to display or delete DNSKEY records. This is a required field.

- **owner**
  Specifies a domain name on which to filter the DNSKEY records in the specified DNS cache for a query or deletion.

- **slot**
  Specifies a slot number on a chassis that contains the specified DNS cache. This is a one-based index.

- **tmm**
  Specifies the number of the TMM that contains the specified DNS cache. Use this option only for debugging. This is a zero-based index.

## See also

`delete`, `show`, `tmsh`
msg

Manages message records in the DNS caches on the BIG-IP system.

Module

ltm dns cache records

Syntax

Configure the msg component within the ltm dns cache records module using the following syntax.

Display

show msg cache [cache name]

options:
    qname [domain name]
    rcode [integer]
    slot [integer]
    tmm [integer]

Delete

delete msg cache [cache name]

options:
    qname [domain name]
    rcode [integer]
    slot [integer]
    tmm [integer]

Description

The msg component contains full DNS messages. You can display and delete these messages.

Examples

Displays the message records in the DNS cache named resolver_cache:
show msg cache resolver_cache

Deletes the message records from the DNS cache named v_resolver_cache:
delete msg cache v_resolver_cache
Options

You can use the following options with the `msg` component:

- **cache name**
  Specifies a DNS cache from which to display or delete DNS messages. This is a required field.

- **qname**
  Specifies a domain name on which to filter the DNS messages in the specified DNS cache for a query or deletion.

- **rcode**
  Specifies the DNS return code on which to filter DNS messages in the specified DNS cache for a query or deletion.

- **slot**
  Specifies a slot number on a chassis that contains the specified DNS cache. This is a one-based index.

- **tmm**
  Specifies the number of the TMM that contains the specified DNS cache. This is a zero-based index.

See also

delete, show, tmsh
nameserver

Manages nameserver records in the DNS cache resolvers on the BIG-IP system.

Module

ltm dns cache records

Syntax

Configure the nameserver component within the ltm dns cache records module using the following syntax.

Display

show cache [cache name]
  options:
    address [ip address]
    has-edns [yes | no]
    has-lame [yes | no]
    rtt-range [min:max]
    slot [integer]
    tmm [integer]
    ttl-range [min:max]
    zone-name [name]

Delete

delete cache [cache name]
  options:
    address [ip address]
    has-edns [yes | no]
    has-lame [yes | no]
    rtt-range [min:max]
    slot [integer]
    tmm [integer]
    ttl-range [min:max]
    zone-name [name]
Description

You can use the nameserver component to display or delete nameserver records from a DNS cache. The maximum number of records returned is 1000; therefore, broad searches cannot show all records in the cache.

Examples

Displays the nameserver records in the DNS cache named my_cache with the zone name com, where the TTLs of the records are between 50 and 500:

```
show cache my_cache zone-name com ttl-range 50:500
```

Options

You can use these options with the nameserver component:

- **address**
  Specifies the nameserver records in the specified DNS cache to select based on the IP address of the nameserver.

- **cache name**
  Specifies a DNS cache name. This is a required field.

- **has-edns**
  Specifies the nameserver records to select from the specified DNS cache, based on whether the nameserver is EDNS lame. An EDNS lame nameserver does not reply to EDNS queries.

- **has-lame**
  Specifies the nameserver records to select from the specified DNS cache, based on whether the nameserver is lame for one or more items.

- **rtt-range**
  Specifies the nameserver records to select from the specified DNS cache based on RTTs within the specified range (inclusive). A missing value (:500 or 50:) defaults to the minimum or maximum, respectively.

- **slot**
  Specifies a slot number on a chassis that contains the specified DNS cache. This is a one-based index.

- **tmm**
  Specifies the number of the TMM that contains the specified DNS cache. This is a zero-based index.

- **ttl-range**
  Specifies the nameserver records to select from the specified DNS cache, based on TTLs within the specified range (inclusive). A missing value (:500 or 50:) defaults to the minimum or maximum, respectively.

- **zone-name**
  Specifies the nameserver records to select from the specified DNS cache, based on the specified zone name.
See also

delete, show, tmsh
**rrset**

Manages the RRset records in the DNS cache resolvers on the BIG-IP system.

**Module**

**ltm dns cache records**

**Syntax**

Configure the `rrset` component within the `ltm dns cache records` module using the syntax in the following sections.

**Display**

`show cache [cache name]`

```
options:
  class [IN | CH | HS | ANY]
  owner [DNS name]
  slot [integer]
  tmm [integer]
  ttl-range [integer:integer]
  type type [A | AAAA | CNAME | NS | PTR | RRSIG | DNSKEY | SOA | TXT | ANY | ... ]
```

**Delete**

`delete cache [cache name]`

```
options:
  class [IN | CH | HS | ANY]
  owner [DNS name]
  slot [integer]
  tmm [integer]
  ttl-range [integer:integer]
  type type [A | AAAA | CNAME | NS | PTR | RRSIG | DNSKEY | SOA | TXT | ANY | ... ]
```

**Description**

You can use the `rrset` component to display or delete records in the specified DNS cache. The maximum number of records returned is 1000. Broad searches might not show all records in the cache.
Examples

Displays RRset records of type A, class IN, with TTLs between 20 and 5000, and an owner of .com:

```
show cache resCache2 class IN type A ttl-range 20:5000 owner .com
```

Options

You can use the following options with the `rrset` component:

- **cache name**
  Specifies a DNS cache name. This is a required field.

- **class**
  Specifies the class of RRset records to select from the specified DNS cache.

- **owner**
  Specifies the node on which to filter the RRset records in the specified DNS cache for a query or deletion.

- **slot**
  Specifies a slot number on a chassis that contains the specified DNS cache. This is a one-based index.

- **tmm**
  Specifies the number of the TMM that contains the specified DNS cache. This is a zero-based index.

- **ttl-range**
  Specifies the RRset records to select from the specified DNS cache, based on TTLs within the specified range (inclusive). A missing value (:500 or 50:) defaults to the minimum or maximum, respectively.

- **type**
  Specifies the RRset records to select from the specified DNS cache, based on the specified type. Most record types are supported.

See also

`delete`, `show`, `tmsh`
Introducing the Ltm dns dns-express module

Alphabetical list of components
Introducing the ltm dns dns-express module

You can use the tmsh components that reside within the ltm dns dns-express module to configure settings for accelerating a DNS authoritative name server deployment (BIND running on BIG-IP®).

For information about the tmsh hierarchical structure, see Chapter 2, Understanding and Using the Traffic Management Shell.

Alphabetical list of components

The remainder of this chapter lists the tmsh components that are available in the ltm dns dns-express module.
db

Loads the DNS Express data file.

Module

ltm dns dns-express

Syntax

Configure the `db` component within the `ltm dns dns-express` module using the following syntax.

```
load db
```

Description

You can use the `db` component within the `ltm dns dns-express` module to load DNS Express data files into the system. The files are located in `/var/db/`.

Loading Behavior

When you load DNS Express data files, the system looks for the database file in `/var/db/` and loads it if modifications have been made.

Examples

Loads the DNS Express file from disk into the running configuration:

```
load db
```

See also

`load`, `tmsh`
tsig-key

Configures DNS Express TSIG keys on the BIG-IP system.

Module

**ltm dns dns-express**

Syntax

Configure the **tsig-key** component within the **ltm dns dns-express** module using the following syntax.

Create/Modify

create tsig-key [name]
modify tsig-key [name]

options:

  algorithm [ hmacmd5 | hmacsha1 | hmacsha256 ]
  secret [string]

edit tsig-key [ [ [name] | [glob] | [regex] ] ... ]

options:

  all-properties
  non-default-properties

Display

list tsig-key

list tsig-key [ [ [name] | [glob] | [regex] ] ... ]

options:

  all-properties
  non-default-properties
  one-line

Delete

delete tsig-key [name]

Description

You can use the **tsig-key** component to configure DNS Express TSIG keys and to view information about the keys.
Examples

Creates the TSIG key, **myKey**, given the algorithm and secret (both required):

```
create tsig-key myKey algorithm hmacmd5 secret ABCDEFG
```

Displays the properties of the DNS Express TSIG key **myKey**:

```
list tsig-key myKey
```

Options

You can use the following options with the *kerberos-delegation* component:

- **algorithm**
  Specifies the algorithm to use to generate the key.

- **glob**
  Displays the items that match the *glob* expression. See `help glob` for a description of *glob* expression syntax.

- **name**
  Specifies a unique name for the component. This option is required for the commands `create`, `delete`, and `modify`.

- **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@\[regular expression\]) to indicate that the identifier is a regular expression. See `help regex` for a description of regular expression syntax.

- **secret**
  Specifies the string representation of the key's shared secret.

See also

- `create`, `delete`, `edit`, `glob`, `list`, `modify`, `regex`, `tmsh`
zone

Configures DNS Express zones on the BIG-IP system.

Module

ltm dns dns-express

Syntax

Configure the zone component within the ltm dns dns-express module using the following syntax.

Create/Modify

create zone [name]
modify zone [name]
options:
  [enabled | disabled]
  notify-action [ consume | bypass | repeat ]
  transfer-target [ip address]
  transfer-tsig-key [tsig-key name]
edit zone [ [ [name] | [glob] | [regex] ] ... ]
options:
  all-properties
  non-default-properties

Display

list zone
list zone [ [ [name] | [glob] | [regex] ] ... ]
options:
  all-properties
  non-default-properties
  one-line
  show zone [name]

Delete

delete zone [name]

Description

You can use the zone component to configure and view information about a DNS Express zone.
Examples

Displays the properties of the DNS Express zone named `myZone`:

```
list zone myZone
```

Options

You can use these options with the `ldap` component:

- **name**
  Specifies a unique name for the component. This option is required for the commands `create`, `delete`, and `modify`.

- **[enabled | disabled]**
  Specifies whether the DNS Express zone is *enabled* or *disabled*.
  *Note:* A successful zone transfer must occur before this zone can service DNS requests.

- **glob**
  Displays the items that match the *glob* expression. See `help glob` for a description of *glob* expression syntax.

- **notify-action [ consume | bypass | repeat ]**
  Action to take when a NOTIFY query is received for a configured zone. Options are `consume`, `bypass`, and `repeat`.
  - **Default** is `consume`, meaning the NOTIFY query is seen only by DNS-Express.
  - **bypass** means the query will NOT go to DNS-Express, but any backend DNS resource (subject to DNS profile `unhandled-query-action`).
  - **repeat** means the NOTIFY will go to both DNS-Express and any backend DNS resource. If TSIG is configured, the signature is only validated for `consume` and `repeat` actions.
  - NOTIFY responses are assumed to be sent by the backend DNS resource, except when the action is `consume` and DNS-Express will generate a response.

- **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. See `help regex` for a description of regular expression syntax.

- **transfer-target [ip address]**
  Specifies the IP address of a Master DNS server to initiate a zone transfer from.

- **transfer-tsig-key [tsig-key name]**
  Specifies the name of an existing TSIG key on the BIG-IP® system to use when processing the zone transfer.
See also

create, delete, edit, glob, list, modify, regex, show, tmsh
Ltm dns dnssec Module Components

- Introducing the Ltm dns dnssec module
- Alphabetical list of components
Introducing the ltm dns dnssec module

You can use the tmsh components that reside within the ltm dns dnssec module to configure components that enable DNS security extensions.

For information about the tmsh hierarchical structure, see Chapter 2, *Understanding and Using the Traffic Management Shell*.

Alphabetical list of components

The remainder of this chapter lists the tmsh components that are available in the ltm dns dnssec module.
**Generation**

Configures a generation on the BIG-IP® system.

**Module**

ltm dns dnssec

**Syntax**

Configure the generation component within the ltm dns dnssec module using the syntax in the following sections.

**Create/Modify**

modify generation [name]

options:
- expiration [date and time]
- rollover [date and time]

edit generation [ [name] | [glob] | [regex] ] ...

options:
- all-properties
- non-default-properties

**Display**

list generation

list generation [ [name] | [glob] | [regex] ] ...

options:
- all-properties
- non-default-properties
- pub-text

show generation

show generation [ [name] | [glob] | [regex] ] ...

options:
- (default | exa | gig | kil | meg | peta | raw | tera | yotta | zetta)

**Delete**

delete generation [name]

**Description**

You can use the generation component to configure a generation.
Examples

Displays the properties of the generation named `myfirstgen`:

```
list generation myfirstgen
```

Displays the status of the generation named `myfirstgen`:

```
show generation myfirstgen
```

Options

You can use the following options with the generation component:

- **expiration**
  Specifies the date and time that this generation expires.

- **glob**
  Displays the items that match the glob expression. See help `glob` for a description of glob expression syntax.

- **name**
  Specifies a unique name for the component. This option is required for the commands `create`, `delete`, and `modify`.

- **pub-text**
  Displays public text generated by the system.

- **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. See help `regex` for a description of regular expression syntax.

- **rollover**
  Specifies the date and time that this generation rolls over to a new generation.

See also

`create`, `delete`, `edit`, `glob`, `list`, `modify`, `regex`, `show`, `tmsh`
Chapter 29

key

Configures DNSSEC keys on the BIG-IP system.

Module

ltm dns dnssec

Syntax

Configure the key component within the ltm dns dnssec module using the following syntax.

Create/Modify

create key [name]
modify key [name]

options:
  algorithm [ rsasha1 | rsasha256 | rsasha512 ]
  bitwidth [ 512 | 1024 | 2048 | 4096 ]
  description [string]
  [enabled | disabled]
  expiration-period [integer]
  key-type [ksk | zsk]
  rollover-period [integer]
  signature-pub-period [integer]
  signature-valid-period [integer]
  ttl [integer]
  use-fips [no | yes]

edit key [ [ [name] | [glob] | [regex] ] ... ]

options:
  all-properties
  non-default-properties

Display

list key
list key [ [ [name] | [glob] | [regex] ] ... ]

options:
  all-properties
  generation
  non-default-properties
  one-line
Delete

```
delete key [name]
```

Description

You can use the `key` component to configure DNSSEC zone signing and key signing keys, and to view information about the keys.

Examples

Creates the key signing key, `ksk1`, using the system default values:

```
create key ksk1
```

Creates the zone signing key, `zsk1`, using the system default values:

```
create key zsk1
```

Displays the properties of the DNS security key `my_key`.

```
list key my_key
```

Options

You can use these options with the `key` component:

- **algorithm**
  Specifies the algorithm to use to generate the key. The default value is `RSASHA1`.

- **bitwidth**
  Specifies the length of the key you want to generate. The default value is `1024`.

- **description**
  User-defined description.

- **[enabled | disabled]**
  Specifies whether the key is `enabled` or `disabled`.

- **expiration-period**
  Specifies the life of the key in `d:h:m:s`, `h:m:s`, `m:s`, or seconds. At the end of the period, the system deletes the expired generation of the key. This value must be greater than the value of the `rollover-period` option. The difference between the two periods must be more than the value of the `ttl` option.
  The default value is `0` (zero), which indicates unset, and thus the key does not expire.

- **generation**
  Displays the generation of the key, including the following:
  - **creator**
    Hostname of BIG-IP system that created this generation.
• **expiration**
  The date and time that this generation of the key expires.

• **handle**
  The key generation's handle for interacting with the key subsystem (for example, HSM for FIPS).

• **key-tag**
  The hash identifier of the DNSKEY.

• **pub-text**
  The text of the randomly-generated public key.

• **rollover**
  The date and time that this generation of the key rolls over to a new key.

◆ **glob**
  Displays the items that match the glob expression. See help glob for a description of glob expression syntax.

◆ **key-type**
  Specifies whether the key is of type ksk or zsk. The default value is zsk.

◆ **name**
  Specifies a unique name for the component. This option is required for the commands create, delete, and modify.

◆ **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. See help regex for a description of regular expression syntax.

◆ **rollover-period**
  Specifies the amount of time, in d:h:m:s, h:m:s, m:s, or seconds, before the system generates another generation of the key. At the end of the period, the system creates a new generation of the key. Two generations of the key exist during the time between the end of the rollover period and the end of the expiration period.

  This value must be greater than or equal to one third of the value of the expiration-period option, and less than the value of the expiration period option. The difference between the two periods must be greater than the value of the ttl option.

  The default value is 0 (zero), which indicates unset, and thus the key does not roll over.

◆ **signature-pub-period**
  Specifies the amount of time, in d:h:m:s, h:m:s, m:s, or seconds, before the system publishes another generation of the signature. At the end of the period, the system creates a new signature.

  This value must be less than the value of the signature-valid-period option. The default value is 403200 seconds.
◆ **signature-valid-period**
  Specifies the amount of time, in d:h:m:s, h:m:s, m:s, or seconds, that the signature is valid. At the end of the period, the Global Traffic Manager™ no longer uses the expired signature. The default value is 604800 seconds.

◆ **ttl**
  Specifies the amount of time, in d:h:m:s, h:m:s, m:s, or seconds, that a DNS server can cache the key. The default value is 86400.
  The value of the **ttl** option must be less than the difference between the values of the **rollover-period** and **expiration-period** options.
  0 seconds indicates that the key is not cached.

◆ **use-fips**
  Specifies whether to store this key in the FIPS device. The default value is **no**.
  If you set this option to **yes**, and the system does not contain a FIPS card, the system automatically resets the value to **no**.

**See also**

create, delete, edit, glob, list, modify, regex, tmsh
zone

Configures DNSSEC zones on the BIG-IP system.

Module

ltm dns dnssec

Syntax

Configure the zone component within the ltm dns dnssec module using the following syntax.

Create/Modify

create zone [name]
modify zone [name]
  options:
    description [string]
    [enabled | disabled]
    ds-algorithm [ SHA1 | SHA256 ]
    keys
      [add | delete | modify | replace-all-with] {
        [key name ...]
      }
    keys none
    nsec3-algorithm [ SHA1 | SHA256 ]

edit zone [ [ [name] | [glob] | [regex] ] ... ]
  options:
    all-properties
    non-default-properties

Display

list zone
list zone [ [ [name] | [glob] | [regex] ] ... ]
  options:
    all-properties
    non-default-properties
    one-line

Delete

delete zone [name]
Description

You can use the `zone` component to configure and view information about a DNSSEC zone.

Examples

Displays the properties of the DNSSEC zone named `mySecureZone`:

```
list zone mySecureZone
```

Options

You can use these options with the `zone` component:

- **description**
  User-defined description.

- **ds-algorithm**
  Specifies the hash algorithm to use when creating the Delegation Signer (DS) resource record. The default value is `SHA256`.

- **[enabled | disabled]**
  Specifies whether the DNSSEC zone is `enabled` or `disabled`.
  
  *Note:* You must associate both a key signing and a zone signing key with the zone before complete signing of client requests can occur.

- **glob**
  Displays the items that match the `glob` expression. See `help glob` for a description of `glob` expression syntax.

- **keys**
  Specifies the keys that you want to configure for the zone.

- **name**
  Specifies a unique name for the component. This option is required for the commands `create`, `delete`, and `modify`.

- **nsec3-algorithm**
  Specifies the hash algorithm to use when creating the Next Secure (NSEC3) resource record. The default value is `SHA1`.

- **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. See `help regex` for a description of regular expression syntax.

See also

```
create, delete, edit, glob, list, modify, regex, tmsh
```
30

Itm global-settings Module Components

- Introducing the Itm global-settings module
- Alphabetical list of components
Introducing the ltm global-settings module

You can use the tmsh components that reside within the ltm global-settings module to configure global settings for Local Traffic Manager™. For more information about the tmsh hierarchical structure, see Chapter 2, Understanding and Using the Traffic Management Shell.

Alphabetical list of components

The remainder of this chapter lists the tmsh components that are available in the ltm global-settings module.
Chapter 30

connection

Configures the global settings that pertain to connections for the BIG-IP® and VIPRION® Local Traffic Manager™ systems.

Module

ltm global-settings

Syntax

Configure the connection component within the ltm global-settings module using the following syntax.

Modify

modify connection
  options:
    adaptive-reaper-hiwater [integer]
    adaptive-reaper-lowater [integer]
    auto-last-hop [disabled | enabled]
    syncookies-threshold [integer]
    vlan-keyed-conn [disabled | enabled]

Display

list connection
list connection [option name]
show running-config connection
show running-config connection [option name]
  options:
    all-properties
    non-default-properties
    one-line

Description

You can use the connection component to modify how the system processes connections.
Examples

Specifies that the system does not automatically map the last hop for pools:

```
modify connection auto-last-hop disabled
```

Displays the global settings for how the system processes connections:

```
list connection
```

Options

You can use these options with the `connection` component:

- **adaptive-reaper-hiwater**
  Specifies, in percent, the memory usage at which the system stops establishing new connections. Once the system meets the reaper high-water mark, the system does not establish new connections until the memory usage drops below the reaper low-water mark. The adaptive reaper settings help mitigate the effects of a denial-of-service attack.

  The available range is **85** - **100**. The default value is **95**. To disable the adaptive reaper, set the high-water mark to **100**.

- **adaptive-reaper-lowater**
  Specifies, in percent, the memory usage at which the system silently purges stale connections, without sending reset packets (RST) to the client. If the memory usage remains above the low-water mark after the purge, then the system starts purging established connections closest to their service timeout.

  The available range is **70** - **100**. The default value is **85**. To disable the adaptive reaper, set the low-water mark to **100**.

- **auto-last-hop**
  Specifies that the system automatically maps the last hop for pools. The default value is **enabled**.

- **syncookies-threshold**
  Specifies the number of new or untrusted TCP connections that can be established before the system activates the SYN Cookies authentication method for subsequent TCP connections. The default value is **16384**.

- **vlan-keyed-conn**
  Enables or disables VLAN-keyed connections. You use VLAN-keyed connections when traffic for the same connection must pass through the system several times on multiple pairs of VLANs (or in different VLAN groups). The default value is **enabled**.

See also

```
list, ltm node, modify, show, tmsh
```
Chapter 30

general

Configures the general properties for the BIG-IP and VIPRION Local Traffic Manager systems.

Module

ltm global-settings

Syntax

Configure the general component within the ltm global-settings module using the following syntax.

Modify

modify general
  options:
    l2-cache-timeout [ integer value: 0 - 2147483647]
    maintenance-mode [disabled | enabled]
    share-single-mac [first-member | global]
    snat-packet-forward [ disabled | enabled]

Display

list general
list general [option name]
show running-config general
show running-config general [option name]
  options:
    all-properties
    non-default-properties
    one-line

Description

You can use the general component to modify how the system processes local traffic.
Examples

Places the Local Traffic Manager™ system in maintenance mode:
modify general maintenance-mode enabled

Displays the general properties of the Local Traffic Manager system:
list general

Options

You can use these options with the nat component:

- **l2-cache-timeout**
  Specifies, in seconds, the amount of time that records remain in the Layer 2 forwarding table, when the MAC address of the record is no longer detected on the network.
  The default value is 300 seconds. The range is 0 (zero) to 2147483647 seconds.

- **maintenance-mode**
  Specifies, when enabled, that the unit is in maintenance mode. In maintenance mode, the system stops accepting new connections and slowly finishes off existing connections.
  The default value is disabled.

- **share-single-mac**
  Specifies the Media Access Control address (MAC address) that the system assigns to a VLAN. The default value is first-member, which indicates that a VLAN uses the MAC address of its first unused member. The global value indicates that all of the VLANs on the system use the same MAC address.

- **snat-packet-forward**
  Enables or disables SNAT packet forwarding. The default value is enabled.

See also

list, ltm node, modify, show, tmsh
traffic-control

Configures the global settings that pertain to traffic control for the BIG-IP and VIPRION Local Traffic Manager systems.

Module

ltm global-settings

Syntax

Configure the traffic-control component within the ltm global-settings module using the following syntax.

Modify

modify traffic-control

options:
   accept-ip-options [disabled | enabled]
   accept-ip-source-route [disabled | enabled]
   allow-ip-source-route [disabled | enabled]
   continue-matching [disabled | enabled]
   max-icmp-rate [integer value: 0 - 2147483647]
   max-reject-rate [integer value: 1 - 1000]
   min-path-mtu [integer value: 68 - 1500]
   path-mtu-discovery [disabled | enabled]
   port-find-linear [integer value: 0 - 61439]
   port-find-random [integer value: 0 - 1024]
   reject-unmatched [disabled | enabled]

Display

list traffic-control
list traffic-control [option name]
show running-config traffic-control
show running-config traffic-control [option name]

options:
   all-properties
   non-default-properties
   one-line
Description

You can use the `traffic-control` component to modify how the system processes local traffic.

Examples

Specifies that the system accepts IPv4 packets with IP options:
```
modify traffic-control accept-ip-options enabled
```

Displays the local traffic control global settings:
```
list traffic-control
```

Options

You can use these options with the `traffic-control` component:

- **accept-ip-options**
  Specifies whether the system accepts IPv4 packets with IP options. The default value is `disabled`.

- **accept-ip-source-route**
  Specifies whether the system accepts IPv4 packets with IP source route options that are destined for Traffic Management Microkernel (TMM). The default value is `disabled`.
  To enable this option, you must also enable the `accept-ip-options` option.

- **allow-ip-source-route**
  Specifies whether the system allows IPv4 packets with IP source route options enabled to be routed through Traffic Management Microkernel (TMM). The default value is `disabled`.
  To enable this option, you must also enable the `accept-ip-options` option.

- **continue-matching**
  Specifies whether the system matches against a less-specific virtual server when the more-specific one is disabled. When `continue-matching` (the default value) is `disabled`, the system drops connections that request a disabled virtual server. In this case, the system rejects or drops packets depending on the value of the `reject-unmatched` option.

- **max-icmp-rate**
  Specifies the maximum rate per second at which the system issues Internet Control Message Protocol (ICMP) errors. The default value is **100** errors per second. The range is from **0** (zero) to **2147483647** errors per second. This option is useful for preventing ICMP-message storms.

- **max-reject-rate**
  Specifies the maximum rate per second at which the system issues reject packets (TCP RST or ICMP port unreachable). The default value is **250** per second. The range is from **1** to **1000** per second.
◆ **min-path-mtu**
   Specifies the minimum packet size that can traverse the path without suffering fragmentation, also known as path Maximum Transmission Unit (MTU). The default value is 296. The range is from 68 to 1500.

◆ **path-mtu-discovery**
   Specifies, when enabled, that the system discovers the maximum transmission unit (MTU) that it can send over a path, without fragmenting TCP packets. The default value is **enabled**.

◆ **port-find-linear**
   Specifies the maximum of ports to linearly search for outbound connections. The default is 16. The range is from 0 to 61439.

◆ **port-find-random**
   Specifies the maximum of ports to randomly search for outbound connections. The default is 16. The range is from 0 to 1024.

◆ **reject-unmatched**
   Specifies, when enabled, that the system returns a TCP RESET or ICMP_UNREACH packet if no virtual servers on the system match the destination address of the incoming packet. When this option is disabled, the system silently drops the unmatched packet. The default value is **enabled**.

**See also**

list, ltm node, modify, show, tmsh
Ltm monitor Module Components

- Introducing the Ltm monitor module
- Alphabetical list of components
Introducing the ltm monitor module

You can use the tmsh components that reside within the ltm monitor module to configure Local Traffic Manager™ monitors. For more information about the tmsh hierarchical structure, see Chapter 2, Understanding and Using the Traffic Management Shell.

For more information about configuring monitors, refer to the Configuration Guide for BIG-IP® Local Traffic Manager™.

Alphabetical list of components

The remainder of this chapter lists the tmsh components that are available in the ltm monitor module.
**diameter**

Configures a monitor for Diameter protocol resources.

**Module**

**ltm monitor**

**Syntax**

Configure the `diameter` component within the `ltm monitor` module using the following syntax.

**Create/Modify**

```
create diameter [name]
modify diameter [name]
```

Options:

- `acct-application-id` [integer] | none
- `auth-application-id` [integer] | none
- `defaults-from` [name]
- `description` [string]
- `host-ip-address` [ip address] | none
- `interval` [integer]
- `manual-resume` [enabled | disabled]
- `origin-host` [ip address] | none
- `origin-realm` [hostname] | none
- `product-name` [name]
- `time-until-up` [integer]
- `timeout` [integer]
- `up-interval` [integer]
- `vendor-id` [integer]
- `vendor-specific-acct-application-id` [integer] | none
- `vendor-specific-auth-application-id` [integer] | none
- `vendor-specific-vendor-id` [integer] | none

```
edit diameter [name | glob | regex] ...
edit diameter [name | glob | regex] ...
```

Options:

- `all-properties`
- `non-default-properties`

**Display**

```
list diameter
list diameter [name | glob | regex] ...
```

show running-config diameter
show running-config diameter [ [[name] | [glob] | [regex] ] ... ]
  options:
    all-properties
    non-default-properties
    one-line
    partition

Delete

delete diameter [name]

◆ Note

You cannot delete default monitors.

Description

You can use the `diameter` component to configure a custom monitor, or you can use the default Diameter monitor that Local Traffic Manager provides. This type of monitor checks the health of Diameter protocol resources.

Examples

Creates a monitor named `my_diameter` that inherits properties from the default Diameter monitor.

```
create diameter my_diameter defaults-from diameter
```

Displays the properties of all of the Diameter monitors:

```
list diameter
```

Options

You can use these options with the `diameter` component:

◆ `acct-application-id`
  Specifies the ID of the accounting portion of a Diameter application. If you specify this option, you must also specify a value for the `auth-application-id` option. The default value is `none`.

  *Note: The `acct-application-id` and `auth-application-id` attribute-value-pair (AVP), and the `vendor-specific-auth-application-id` and `vendor-specific-acct-application-id` AVP are mutually exclusive. You can only specify one set of these AVPs.*
◆ **auth-application-id**
  Specifies the ID of the authentication and authorization portion of a Diameter application. If you specify this option, you must also specify a value for the **acct-application-id** option. The default value is **none**.

  *Note: The acct-application-id and auth-application-id attribute-value-pair (AVP), and the vendor-specific-auth-application-id and vendor-specific-acct-application-id AVP are mutually exclusive. You can only specify one set of these AVPs.*

◆ **defaults-from**
  Specifies the name of the monitor from which you want your custom monitor to inherit settings. The default value is **diameter**.

◆ **description**
  User-defined description.

◆ **glob**
  Displays the items that match the **glob** expression. For a description of **glob** expression syntax, see the **glob** man page.

◆ **host-ip-address**
  Specifies the IP address of the sender of the Diameter message for the Diameter protocol peer discovery feature. The default value is **none**.

◆ **interval**
  Specifies, in seconds, the frequency at which the system issues the monitor check when either the resource is **down** or the status of the resource is unknown. The default value is **10** seconds.

◆ **manual-resume**
  Specifies whether the system automatically changes the status of a resource to **up** at the next successful monitor check. The default value is **disabled**.

  *Note: If you set the manual-resume option to enabled, you must manually mark the resource as up before the system can use it for load balancing connections.*

◆ **name**
  Specifies a unique name for the component. This option is required for the commands **create**, **delete**, and **modify**.

◆ **origin-host**
  Specifies the IP address from which the Diameter message originates. The default value is **none**.

◆ **origin-realm**
  Specifies the realm in which the host from which the Diameter message originates resides. The default value is **f5.com**.

◆ **partition**
  Displays the administrative partition in which the component resides.

◆ **product-name**
  Specifies the vendor-assigned name of the Diameter application. The value of this option must remain constant across firmware revisions for the same product. The default value is **F5 BIGIP Diameter Health Monitoring**.
◆ **regex**
   Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. For a description of regular expression syntax, see the `regex` man page.

◆ **time-until-up**
   Specifies the amount of time in seconds after the first successful response before a node is marked up. A value of 0 (zero) causes a node to be marked up immediately after a valid response is received from the node. The default value is 0 (zero).

◆ **timeout**
   Specifies the number of seconds the target has in which to respond to the monitor request. The default value is 31 seconds.

   If the target responds within the set time period, it is considered **up**. If the target does not respond within the set time period, it is considered **down**. Also, if the target responds with a RESET packet, the system immediately flags the target as **down** without waiting for the timeout interval to expire.

◆ **up-interval**
   Specifies, in seconds, the frequency at which the system issues the monitor check when the resource is **up**. The default value is 0 (zero), which specifies that the system uses the value of the `interval` option whether the resource is **up** or **down**.

   **Important:** F5 Networks recommends that when you configure this option and the `interval` option, that you ensure that the greater value is a multiple of the lesser value, to allow for an even distribution of monitor checks among all monitors.

◆ **vendor-id**
   Specifies the IANA SMI Network Management Private Enterprise Code assigned to the vendor of the Diameter application. The default value is 3375.

◆ **vendor-specific-acct-application-id**
   Specifies the ID of the vendor-specific accounting portion of a Diameter application. If you specify this option, you must also specify a value for the `vendor-specific-auth-application-id` option. The default value is **none**.

   **Note:** The `acct-application-id` and `auth-application-id` attribute-value-pair (AVP), and the `vendor-specific-auth-application-id` and `vendor-specific-acct-application-id` AVP are mutually exclusive. You can only specify one set of these AVPs.
◆ vendor-specific-auth-application-id
   Specifies the ID of the vendor-specific authentication and authorization
   portion of a Diameter application. If you specify this option, you must
   also specify a value for the vendor-specific-acct-application-id option.
   The default value is none.

   Note: The acct-application-id and auth-application-id
   attribute-value-pair (AVP), and the vendor-specific-auth-application-id
   and vendor-specific-acct-application-id AVP are mutually exclusive. You
   can only specify one set of these AVPs.

◆ vendor-specific-vendor-id
   Specifies the ID of a vendor-specific Diameter application. The system
   uses this ID to advertise support for the application. The default value is
   none.

See also

create, delete, edit, glob, list, modify, regex, show, tmsh
dns

Configures a Domain Name System (DNS) monitor.

Module

ltm monitor

Syntax

Configure the dns component within the ltm monitor module using the syntax in the following sections.

Create/Modify

create dns [name]
modify dns [name]
  options:
    accept-rcode [no-error | anything]
    answer-contains [query-type | any-type | anything]
    defaults-from [name]
    description [string]
    destination [ip address][port]
    interval [integer]
    manual-resume [enabled | disabled]
    qname [string]
    qtype [a | aaaa]
    recv [none | [string] ]
    reverse [enabled | disabled]
    time-until-up [integer]
    timeout [integer]
    transparent [disabled | enabled]
    up-interval [integer]
edit dns [ [ [name] | [glob] | [regex] ] ... ]
  options:
    all-properties
    non-default-properties

Display

list mysql
list mysql [ [ [name] | [glob] | [regex] ] ... ]
show running-config mysql
show running-config mysql  [ [ [name] | [glob] | [regex] ] ... ]
  options:
    all-properties
    non-default-properties
    one-line
    partition

Delete

delete dns [name]

◆ Note

You cannot delete default monitors.

Description

You can use the dns component to configure a custom monitor. This type of monitor verifies the DNS service by attempting to send DNS requests generated using the parameters provided to a pool, pool member, or virtual server and validating the DNS response.

Examples

Creates a monitor named my_mysql that inherits properties from the default MySQL monitor.

create dns my_dns defaults-from dns qname www.test.com

Displays the properties of all of the DNS monitors:

list dns

Options

You can use these options with the dns component:

♦ acceptrcode
  Specifies the RCODE required in the response for an up status. The default value is no-error. The options are:
  • no-error
    Specifies that the status of the node will be marked up if the received DNS message has RCODE = NOERROR.
  • anything
    Specifies that the status of the node will be marked up irrespective of the RCODE in the DNS message received.
◆ **answer_contains**
  Specifies the record types required in the answer section of the response in order to mark the status of a node **up**. The default value is **query-type**. The options are:
  - **query-type**
    Specifies that the response should contain at least one answer of which the resource record type matches the **qtype**.
  - **any-type**
    Specifies that the DNS message should contain at least one answer.
  - **anything**
    Specifies that an empty answer section is enough to mark the status of the node **up**.

◆ **defaults-from**
  Specifies the name of the monitor from which you want your custom monitor to inherit settings. The default value is **mssql**.

◆ **description**
  User-defined description.

◆ **destination**
  Specifies the IP address and service port of the resource that is the destination of this monitor. The default value is **:***. Possible values are:
  - **:***
    Specifies that the system marks a pool member **up** or **down** based on the response of the server at the IP address and port supplied by the pool member.
  - **:*:<port>**
    Specifies that the system marks a pool member **up** or **down** based on the response of the server at the IP address supplied by the pool member and the port you specify.
  - **<IP address>:<port>**
    Specifies that the system marks a pool member **up** or **down** based on the response of the server at the IP address and port you specify.

◆ **glob**
  Displays the items that match the **glob** expression. For a description of **glob** expression syntax, see the **glob** man page.

◆ **interval**
  Specifies, in seconds, the frequency at which the system issues the monitor check when either the resource is **down** or the status of the resource is unknown. The default value is 30 seconds.

◆ **manual-resume**
  Specifies whether the system automatically changes the status of a resource to **up** at the next successful monitor check. The default value of the **manual-resume** option is **disabled**.
  If you set the **manual-resume** option to **enabled**, you must manually mark the resource as **up** before the system can use it for load balancing connections.
◆ name  
Specifies a unique name for the component. This option is required for the commands create, delete, and modify.

◆ partition  
Displays the administrative partition in which the component resides.

◆ qname  
Specifies the query name that the monitor sends a DNS query for. The default value is Enter a query name.

◆ qtype  
Specifies the query type that the monitor sends a DNS query for. The default value is a. Possible values are:

  • a  
    Specifies that the monitor will send a DNS query of type A.
  
  • aaaa  
    Specifies that the monitor will send a DNS query of type AAAA.

◆ recv  
Specifies the text string that the monitor looks for in the returned resource. The default value is none.

The most common receive expressions contain a text string that is included in a field in your database. If you do not specify a value for both the send and recv options, the monitor performs a simple service check and connect only.

◆ reverse  
Specifies whether the monitor operates in reverse mode. When the monitor is in reverse mode, a successful check marks the monitored object down instead of up. You can use this mode only if you configure recv option. The default value is disabled, which specifies that the monitor does not operate in reverse mode. The enabled value specifies that the monitor operates in reverse mode.

◆ regex  
Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. For a description of regular expression syntax, see the regex man page.

◆ time-until-up  
Specifies the amount of time in seconds after the first successful response before a node is marked up. A value of 0 (zero) causes a node to be marked up immediately after a valid response is received from the node. The default value is 0 (zero).

◆ timeout  
Specifies the number of seconds the target has in which to respond to the monitor request. The default value is 91 seconds.

If the target responds within the set time period, it is considered up. If the target does not respond within the set time period, it is considered down. Also, if the target responds with a RESET packet, the system immediately flags the target as down without waiting for the timeout interval to expire.
- **transparent**
  Specifies whether the monitor operates in transparent mode. Monitors in transparent mode can monitor pool members through firewalls. The default value is **disabled**.

- **up-interval**
  Specifies, in seconds, the frequency at which the system issues the monitor check when the resource is **up**. The default value is 0 (zero), which specifies that the system uses the value of the **interval** option whether the resource is **up** or **down**.

  **Important:** F5 Networks recommends that when you configure this option and the **interval** option, that the value that is greater be a multiple of the lesser value to allow for an even distribution of monitor checks among all monitors.

See also

create, delete, edit, glob, list, modify, regex, show, tmsh
external

Configures an external monitor.

Module

ltm monitor

Syntax

Configure the external component within the ltm monitor module using the following syntax.

Create/Modify

create external [name]
modify external [name]

options:
  args [arguments] | none
  defaults-from [name]
  description [string]
  destination [ip address][port]
  interval [integer]
  manual-resume [enabled | disabled]
  run [none | [path] ]
  time-until-up [integer]
  timeout [integer]
  up-interval [integer]
  user-defined [ [name] [value] | none ]

edit external [ [name] | [glob] | [regex] ] ...

options:
  all-properties
  non-default-properties

Display

list external
list external [ [name] | [glob] | [regex] ] ...

show running-config external
show running-config external [ [[name] | [glob] | [regex]] ] ...

options:
  all-properties
  non-default-properties
  one-line
  partition
Delete

```
delete external [name]
```

◆ Note

You cannot delete default monitors.

Description

You can use the `external` component to configure a custom monitor, or you can use the default external monitor that Local Traffic Manager provides. Using this type of monitor you can use your own programs to monitor services.

Examples

Creates a monitor named `my_external` that inherits properties from the default external monitor.

```
create external my_external defaults-from external
```

Displays the properties of all of the external monitors:

```
list external
```

Options

You can use these options with the `external` component:

◆ `args`
   Specifies any command line arguments that the external program requires. The default value is `none`.

◆ `defaults-from`
   Specifies the name of the monitor from which you want your custom monitor to inherit settings. The default value is `external`.

◆ `description`
   User-defined description.

◆ `destination`
   Specifies the IP address and service port of the resource that is the destination of this monitor. The default value is `*:*`.
   Possible values are:
   - `*:*
     Specifies that the system marks a pool member _up_ or _down_ based on the response of the server at the IP address and port supplied by the pool member.
*:*<port>
Specifies that the system marks a pool member *up* or *down* based on the response of the server at the IP address supplied by the pool member and the port you specify.

* <IP address>:<port>
  Specifies that the system marks a pool member *up* or *down* based on the response of the server at the IP address and port you specify.

- *glob*
  Displays the items that match the *glob* expression. For a description of *glob* expression syntax, see the *glob* man page.

- *interval*
  Specifies, in seconds, the frequency at which the system issues the monitor check when either the resource is *down* or the status of the resource is unknown. The default value is 5 seconds.

- *manual-resume*
  Specifies whether the system automatically changes the status of a resource to *up* at the next successful monitor check. The default value of the *manual-resume* option is *disabled*.
  If you set the *manual-resume* option to *enabled*, you must manually mark the resource as *up* before the system can use it for load balancing connections.

- *name*
  Specifies a unique name for the component. This option is required for the commands *create*, *delete*, and *modify*.

- *partition*
  Displays the administrative partition in which the component resides.

- *regex*
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. For a description of regular expression syntax, see the *regex* man page.

- *run*
  Specifies the path and file name of a program to run as the external monitor, for example /config/monitors/myMonitor. The default value is *none*.

- *time-until-up*
  Specifies the amount of time in seconds after the first successful response before a node is marked up. A value of 0 (zero) causes a node to be marked up immediately after a valid response is received from the node. The default value is 0 (zero).

- *timeout*
  Specifies the number of seconds the target has in which to respond to the monitor request. The default value is 16 seconds.
If the target responds within the set time period, it is considered **up**. If the target does not respond within the set time period, it is considered **down**. Also, if the target responds with a RESET packet, the system immediately flags the target as **down** without waiting for the timeout interval to expire.

- **up-interval**
  Specifies, in seconds, the frequency at which the system issues the monitor check when the resource is **up**. The default value is **0** (zero), which specifies that the system uses the value of the **interval** option whether the resource is **up** or **down**.

  **Important:** F5 Networks recommends that when you configure this option and the **interval** option, that the value that is greater be a multiple of the lesser value to allow for an even distribution of monitor checks among all monitors.

- **user-defined**
  Specifies any user-defined command line arguments and variables that the external program requires.

  Use the following syntax to specify a user defined parameter.

  ```
  modify external my_external user-defined my_param_name my_param_value
  ```

  Use the following syntax to remove a user defined parameter.

  ```
  modify external my_external user-defined my_param_name none
  ```

**See also**

- create, delete, edit, glob, list, modify, regex, show, tmsh
**firepass**

Configures a FirePass® monitor.

**Module**

`ltm monitor`

**Syntax**

Configure the `firepass` component within the `ltm monitor` module using the following syntax.

**Create/Modify**

```
create firepass [name]
modify firepass [name]
options:
cipherlist [string]
concurrency-limit [integer]
defaults-from [name]
description [string]
destination [ip address][port]
interval [integer]
manual-resume [enabled | disabled]
max-load-average [integer]
password [password]
time-until-up [integer]
timeout [integer]
up-interval [integer]
username [ [name] | none]
edit firepass [ [ [name] | [glob] | [regex] ] ... ]
options:
all-properties
non-default-properties
```

**Display**

```
list firepass
list firepass [ [ [name] | [glob] | [regex] ] ... ]
show running-config firepass
show running-config firepass [ [ [name] | [glob] | [regex] ] ... ]
options:
all-properties
```
non-default-properties
one-line
partition

Delete

```
delete firepass [name]
```

◆ Note

You cannot delete default monitors.

Description

You can use the `firepass` component to configure a custom monitor, or you can use the default FirePass monitor that Local Traffic Manager provides. This type of monitor checks the health of FirePass systems.

Examples

Creates a monitor named `my_firepass` that inherits properties from the default FirePass monitor.

```
create firepass my_firepass defaults-from firepass
```

Displays the properties of all of the FirePass monitors:

```
list firepass
```

Options

You can use these options with the `firepass` component:

◆ `cipherlist`
  Specifies a cipher list. If you do not specify a cipher list, the monitor uses the default cipher list `HIGH:!ADH`.

◆ `concurrency-limit`
  Specifies the maximum percentage of licensed connections currently in use under which the monitor marks the FirePass system `up`. As an example, a value of 95 percent means that the monitor marks the FirePass system `up` until 95 percent of licensed connections are in use. When the number of in-use licensed connections exceeds 95 percent, the monitor marks the FirePass system `down`. The default value is 95.

◆ `defaults-from`
  Specifies the name of the monitor from which you want your custom monitor to inherit settings. The default value is `firepass`.

◆ `description`
  User-defined description.
◆ **destination**
Specifications the IP address and service port of the resource that is the destination of this monitor. The default value is `*:*

Possible values are:

- `*: *
  Specifies that the system marks a pool member **up** or **down** based on the response of the server at the IP address and port supplied by the pool member.

- `*: port
  Specifies that the system marks a pool member **up** or **down** based on the response of the server at the IP address supplied by the pool member and the port you specify.

- `<IP address>:<port>
  Specifies that the system marks a pool member **up** or **down** based on the response of the server at the IP address and port you specify.

◆ **glob**
Displays the items that match the **glob** expression. For a description of **glob** expression syntax, see the **glob** man page.

◆ **interval**
Specifies, in seconds, the frequency at which the system issues the monitor check when either the resource is **down** or the status of the resource is unknown. The default value is 5 seconds.

◆ **max-load-average**
Specifies the number that the monitor uses to mark the FirePass system **up** or **down**. The system compares the value of this option to a one-minute average of the FirePass system load. When the FirePass system-load average falls within the specified Max Load Average value, the monitor marks the FirePass system **up**. When the average exceeds the value, the monitor marks the system **down**. The default value is 12.

◆ **name**
Specifies a unique name for the component. This option is required for the commands **create**, **delete**, and **modify**.

◆ **partition**
Displays the administrative partition in which the component resides.

◆ **password**
Specifies the password, if the monitored target requires authentication. The default value is **none**.

◆ **regex**
Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. For a description of regular expression syntax, see the **regex** man page.

◆ **time-until-up**
Specifies the amount of time in seconds after the first successful response before a node is marked up. A value of 0 (zero) causes a node to be marked up immediately after a valid response is received from the node. The default value is 0 (zero).
timeout
Specifies the number of seconds the target has in which to respond to the monitor request. The default value is 16 seconds.
If the target responds within the set time period, it is considered up. If the target does not respond within the set time period, it is considered down. Also, if the target responds with a RESET packet, the system immediately flags the target as down without waiting for the timeout interval to expire.

up-interval
Specifies, in seconds, the frequency at which the system issues the monitor check when the resource is up. The default value is 0 (zero), which specifies that the system uses the value of the interval option whether the resource is up or down.

Important: F5 Networks recommends that when you configure this option and the interval option, that the value that is greater be a multiple of the lesser value to allow for an even distribution of monitor checks among all monitors.

username
Specifies the user name if the monitored target requires authentication. The default value is gtmuser.

See also
create, delete, edit, glob, list, modify, regex, show, tmsh
*ftp*

Configures a File Transfer Protocol (FTP) monitor.

**Module**

*ltm monitor*

**Syntax**

Configure the *ftp* component within the *ltm monitor* module using the following syntax.

**Create/Modify**

create ftp [name]

modify ftp [name]

options:
- debug [no | yes]
- defaults-from [name]
- description [string]
- destination [ip address][port]
- filename [ [filename] | none]
- interval [integer]
- manual-resume [enabled | disabled]
- mode [passive | port]
- password [none | [password] ]
- time-until-up [integer]
- timeout [integer]
- up-interval [integer]
- username [name]

edit ftp [ [ [name] | [glob] | [regex] ] ... ]

options:
- all-properties
- non-default-properties

**Display**

list ftp

list ftp [ [ [name] | [glob] | [regex] ] ... ]

show running-config ftp

show running-config ftp [ [ [name] | [glob] | [regex] ] ... ]

options:
- all-properties
non-default-properties
one-line
partition

Delete

delete ftp [name]

◆ Note

You cannot delete default monitors.

Description

You can use the ftp component to configure a custom monitor, or you can use the default FTP monitor that Local Traffic Manager provides. This type of monitor verifies the FTP service by attempting to download a specific file to the /var/tmp directory on the system. Once downloaded successfully, the file is not saved.

Examples

Creates a monitor named my_ftp that inherits properties from the default FTP monitor.

create ftp my_ftp defaults-from ftp

Displays the properties of all of the FTP monitors:

list ftp

Options

You can use these options with the ftp component:

◆ debug

Specifies whether the monitor sends error messages and additional information to a log file created and labeled specifically for this monitor. You can use the log information to help diagnose and troubleshoot unsuccessful health checks. The default value is no.

The options are:

• no

  Specifies that the system does not redirect error messages and additional information related to this monitor.

• yes

  Specifies that the system redirects error messages and additional information to the /var/log/<monitor_type>_<IP address>_<port>.log file.
◆ defaults-from
   Specifies the name of the monitor from which you want your custom monitor to inherit settings. The default value is ftp.

◆ description
   User-defined description.

◆ destination
   Specifies the IP address and service port of the resource that is the destination of this monitor. The default value is *:*.
   Possible values are:
   • *:*  
     Specifies that the system marks a pool member up or down based on the response of the server at the IP address and port supplied by the pool member.
   • *:port  
     Specifies that the system marks a pool member up or down based on the response of the server at the IP address supplied by the pool member and the port you specify.
   • <IP address>:<port>  
     Specifies that the system marks a pool member up or down based on the response of the server at the IP address and port you specify.

◆ filename
   Specifies the full path and file name of the file that the system attempts to download. The health check is successful if the system can download the file. The default value is none.

◆ glob
   Displays the items that match the glob expression. For a description of glob expression syntax, see the glob man page.

◆ interval
   Specifies, in seconds, the frequency at which the system issues the monitor check when either the resource is down or the status of the resource is unknown. The default value is 10 seconds.

◆ manual-resume
   Specifies whether the system automatically changes the status of a resource to up at the next successful monitor check. The default value of the manual-resume option is disabled.
   If you set the manual-resume option to enabled, you must manually mark the resource as up before the system can use it for load balancing connections.

◆ mode
   Specifies the data transfer process (DTP) mode. The default value is passive.
   The options are:
   • passive  
     Specifies that the monitor sends a data transfer request to the FTP server. When the FTP server receives the request, the FTP server then starts and establishes the data connection.
- **port**
  Specifies that the monitor starts and establishes the data connection with the FTP server.

- **name**
  Specifies a unique name for the component. This option is required for the commands `create`, `delete`, and `modify`.

- **password**
  Specifies the password, if the monitored target requires authentication. The default value is `none`.

- **partition**
  Displays the administrative partition in which the component resides.

- **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. For a description of regular expression syntax, see the `regex` man page.

- **time-until-up**
  Specifies the amount of time in seconds after the first successful response before a node is marked up. A value of 0 (zero) causes a node to be marked up immediately after a valid response is received from the node. The default value is 0 (zero).

- **timeout**
  Specifies the number of seconds the target has in which to respond to the monitor request. The default value is 31 seconds.

  If the target responds within the set time period, it is considered **up**. If the target does not respond within the set time period, it is considered **down**. Also, if the target responds with a RESET packet, the system immediately flags the target as **down** without waiting for the timeout interval to expire.

- **up-interval**
  Specifies, in seconds, the frequency at which the system issues the monitor check when the resource is **up**. The default value is 0 (zero), which specifies that the system uses the value of the **interval** option whether the resource is **up** or **down**.

  **Important:** F5 Networks recommends that when you configure this option and the **interval** option, that the value that is greater be a multiple of the lesser value to allow for an even distribution of monitor checks among all monitors.

- **username**
  Specifies the user name if the monitored target requires authentication. The default value is `none`.

---

**See also**

`create`, `delete`, `edit`, `glob`, `list`, `modify`, `regex`, `show`, `tmsh`
**gateway-icmp**

Configures a Gateway Internet Control Message Protocol (ICMP) monitor.

**Module**

`ltm monitor`

**Syntax**

Configure the `gateway-icmp` component within the `ltm monitor` module using the following syntax.

**Create/Modify**

```plaintext
create gateway-icmp [name]
modify gateway-icmp [name]
  options:
    defaults-from [name]
    description [string]
    destination [ip address][port]
    interval [integer]
    manual-resume [enabled | disabled]
    time-until-up [integer]
    timeout [integer]
    transparent [enabled | disabled]
    up-interval [integer]
edit gateway-icmp [ [ [name] | [glob] | [regex] ] ... ]
  options:
    all-properties
    non-default-properties
```

**Display**

```plaintext
list gateway-icmp
list gateway-icmp [ [ [name] | [glob] | [regex] ] ... ]
show running-config gateway-icmp
show running-config gateway-icmp [ [ [name] | [glob] | [regex] ] ... ]
  options:
    all-properties
    non-default-properties
    one-line
    partition
```
Delete

```
delete gateway-icmp [name]
```

◆ Note

*You cannot delete default monitors.*

Description

You can use the `gateway-icmp` component to configure a custom monitor, or you can use the default Gateway ICMP monitor that Local Traffic Manager provides. This type of monitor monitors a pool that implements gateway fail-safe for high availability.

Examples

Creates a monitor named `my_icmp` that inherits properties from the default Gateway ICMP monitor.

```
create gateway-icmp my_icmp defaults-from gateway_icmp
```

Displays the properties of all of the Gateway ICMP monitors:

```
list gateway-icmp
```

Options

You can use these options with the `gateway-icmp` component:

◆ **defaults-from**
  Specifies the name of the monitor from which you want your custom monitor to inherit settings. The default value is `gateway_icmp`.

◆ **description**
  User-defined description.

◆ **destination**
  Specifies the IP address and service port of the resource that is the destination of this monitor. The default value is `*:*`.
  Possible values are:
  - `*:*
    Specifies that the system marks a pool member **up** or **down** based on the response of the server at the IP address and port supplied by the pool member.
  - `*:port
    Specifies that the system marks a pool member **up** or **down** based on the response of the server at the IP address supplied by the pool member and the port you specify.`
• `<IP address>:<port>`
  Specifies that the system marks a pool member **up** or **down** based on the response of the server at the IP address and port you specify.

• `<IP address>:<port>` (with the **transparent** option enabled)
  Specifies that the system performs a health check on the server at the IP address and port you specify, routes the check through the IP address and port supplied by the pool member, and marks the pool member (the gateway) **up** or **down** accordingly.

◆ **glob**
  Displays the items that match the **glob** expression. For a description of **glob** expression syntax, see the **glob** man page.

◆ **interval**
  Specifies, in seconds, the frequency at which the system issues the monitor check when either the resource is **down** or the status of the resource is unknown. The default value is 5 seconds.

◆ **manual-resume**
  Specifies whether the system automatically changes the status of a resource to **up** at the next successful monitor check. The default value of the **manual-resume** option is **disabled**.
  If you set the **manual-resume** option to **enabled**, you must manually mark the resource as **up** before the system can use it for load balancing connections.

◆ **name**
  Specifies a unique name for the component. This option is required for the commands **create**, **delete**, and **modify**.

◆ **partition**
  Displays the administrative partition in which the component resides.

◆ **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. For a description of regular expression syntax, see the **regex** man page.

◆ **time-until-up**
  Specifies the amount of time in seconds after the first successful response before a node is marked up. A value of 0 (zero) causes a node to be marked up immediately after a valid response is received from the node. The default value is 0 (zero).

◆ **timeout**
  Specifies the number of seconds the target has in which to respond to the monitor request. The default value is 16 seconds.
  If the target responds within the set time period, it is considered **up**. If the target does not respond within the set time period, it is considered **down**. Also, if the target responds with a RESET packet, the system immediately flags the target as **down** without waiting for the timeout interval to expire.
• **transparent**
  Specifies whether the monitor operates in transparent mode. Monitors in transparent mode can monitor pool members through firewalls. The default value is **disabled**.

• **up-interval**
  Specifies, in seconds, the frequency at which the system issues the monitor check when the resource is **up**. The default value is **0** (zero), which specifies that the system uses the value of the **interval** option whether the resource is **up** or **down**.

  **Important:** F5 Networks recommends that when you configure this option and the **interval** option, that the value that is greater be a multiple of the lesser value to allow for an even distribution of monitor checks among all monitors.

**See also**

`create`, `delete`, `edit`, `glob`, `list`, `modify`, `regex`, `show`, `tmsh`
http

Configures a Hypertext Transfer Protocol (HTTP) monitor.

Module

ltm monitor

Syntax

Configure the http component within the ltm monitor module using the following syntax.

Create/Modify

create http [name]
modify http [name]
options:
  defaults-from [name]
  description [string]
  destination [ip address][port]
  interval [integer]
  manual-resume [enabled | disabled]
  password [none | [password] ]
  recv [none | [string] ]
  recv-disable [none | [string] ]
  reverse [enabled | disabled]
  send [none | [string] ]
  time-until-up [integer]
  timeout [integer]
  transparent [enabled | disabled]
  up-interval [integer]
  username [ [name] | none]
edit http [ [ [name] | [glob] | [regex] ] ... ]
options:
  all-properties
  non-default-properties

Display

list http
list http [ [name] | [glob] | [regex] ] ... ]
show running-config http
show running-config http [ [name] | [glob] | [regex] ] ... ]
options:
  all-properties
  non-default-properties
  one-line
  partition

Delete

delete http [name]

◆ Note

You cannot delete default monitors.

Description

You can use the http component to configure a custom monitor, or you can use the default HTTP monitor that Local Traffic Manager provides. This type of monitor verifies the HTTP service by attempting to receive specific content from a web page.

Examples

Creates a monitor named my_http that inherits properties from the default HTTP monitor.

create http my_http defaults-from http

Displays the properties of all of the HTTP monitors:

list http

Options

You can use these options with the http component:

◆ defaults-from
  Specifies the name of the monitor from which you want your custom monitor to inherit settings. The default value is http.

◆ description
  User-defined description.
◆ **destination**
   Specifies the IP address and service port of the resource that is the destination of this monitor. The default value is `*:*

   Possible values are:
   
   - `*:*
     Specifies that the system marks a pool member **up** or **down** based on the response of the server at the IP address and port supplied by the pool member.
   
   - `*:port`
     Specifies that the system marks a pool member **up** or **down** based on the response of the server at the IP address supplied by the pool member and the port you specify.
   
   - `<IP address>:<port>`
     Specifies that the system marks a pool member **up** or **down** based on the response of the server at the IP address and port you specify.
   
   - `<IP address>:<port>` (with the `transparent` option **enabled**)
     Specifies that the system performs a health check on the server at the IP address and port you specify, routes the check through the IP address and port supplied by the pool member, and marks the pool member (the gateway) **up** or **down** accordingly.

◆ **glob**
   Displays the items that match the **glob** expression. For a description of **glob** expression syntax, see the **glob** man page.

◆ **interval**
   Specifies, in seconds, the frequency at which the system issues the monitor check when either the resource is **down** or the status of the resource is unknown. The default value is **5** seconds.

◆ **manual-resume**
   Specifies whether the system automatically changes the status of a resource to **up** at the next successful monitor check. The default value of the **manual-resume** option is **disabled**.

   If you set the **manual-resume** option to **enabled**, you must manually mark the resource as **up** before the system can use it for load balancing connections.

◆ **name**
   Specifies a unique name for the component. This option is required for the commands **create**, **delete**, and **modify**.

◆ **partition**
   Displays the administrative partition in which the component resides.

◆ **password**
   Specifies the password if the monitored target requires authentication. The default value is **none**.

◆ **recv**
   Specifies the text string that the monitor looks for in the returned resource. The default value is **none**.
The most common receive expressions contain a text string that is included in an HTML file on your site. The text string can be regular text, HTML tags, or image names. If you do not specify a value for both the send and recv options, the monitor performs a simple service check and connect only.

- **recv-disable**
  Specifies the text string that the monitor looks for in the returned resource. If the text string is matched in the returned resource, the corresponding node or pool member is marked session disabled. The default value is `none`.
  You specify a `recv-disable` string in the same way that you specify a `recv` string.
  If you specify a `recv-disable` string, you must also specify a `recv` string.
  You cannot specify a `recv-disable` string, if the `reverse` option is enabled.

- **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (`@[regular expression]`) to indicate that the identifier is a regular expression. For a description of regular expression syntax, see the `regex` man page.

- **reverse**
  Specifies whether the monitor operates in reverse mode. When the monitor is in reverse mode, a successful check marks the monitored object down instead of up. You can use the this mode only if you configure both the `send` and `recv` options.
  The default value is `disabled`, which specifies that the monitor does not operate in reverse mode. The `enabled` value specifies that the monitor operates in reverse mode.

- **send**
  Specifies the text string that the monitor sends to the target object.
  The default value is `GET /`, which retrieves a default HTML file for a web site. To retrieve a specific page from a web site, specify a fully-qualified path name, for example: `GET /www/company/index.html`.
  Since the string can have special characters, the system requires that the string be enclosed with single quotation marks.
  If this value is null, then a valid connection suffices to determine that the service is up. In this case, the system does not need the `recv` option and ignores the option even if not null.

- **time-until-up**
  Specifies the amount of time, in seconds, after the first successful response before a node is marked up. A value of 0 (zero) causes a node to be marked up immediately after a valid response is received from the node. The default value is 0 (zero).

- **timeout**
  Specifies the number of seconds the target has in which to respond to the monitor request. The default value is 16 seconds.
If the target responds within the set time period, it is considered **up**. If the target does not respond within the set time period, it is considered **down**. Also, if the target responds with a RESET packet, the system immediately flags the target as **down** without waiting for the timeout interval to expire.

- **transparent**
  Specifies whether the monitor operates in transparent mode. Monitors in transparent mode can monitor pool members through firewalls. The default value is **disabled**.

- **up-interval**
  Specifies, in seconds, the frequency at which the system issues the monitor check when the resource is **up**. The default value is **0** (zero), which specifies that the system uses the value of the **interval** option whether the resource is **up** or **down**.

  **Important:** F5 Networks recommends that when you configure this option and the **interval** option, that the value that is greater be a multiple of the lesser value to allow for an even distribution of monitor checks among all monitors.

- **username**
  Specifies the user name if the monitored target requires authentication. The default value is **none**.

**See also**

create, delete, edit, glob, list, modify, regex, show, tmsh
**https**

Configures a Hypertext Transfer Protocol over Secure Socket Layer (HTTPS) monitor.

**Module**

**ltm monitor**

**Syntax**

Configure the `https` component within the `ltm monitor` module using the following syntax.

**Create/Modify**

```
create https [name]
modify https [name]
```

**options:**
- `cert` [cert list] | none
- `cipherlist` [string]
- `compatibility` [enabled | disabled]
- `defaults-from` [name]
- `description` [string]
- `destination` [ip address][port]
- `interval` [integer]
- `key` [key] | none
- `manual-resume` [enabled | disabled]
- `password` [none | [password]]
- `recv` [none | [string]]
- `rec-disable` [none | [string]]
- `reverse` [enabled | disabled]
- `send` [none | [string]]
- `time-until-up` [integer]
- `timeout` [integer]
- `transparent` [enabled | disabled]
- `up-interval` [integer]
- `username` [name] | none

```
edit https [ [name] | [glob] | [regex] ] ...
```

**options:**
- `all-properties`
- `non-default-properties`
Chapter 31

Display

list https
list https [ [ name ] | [ glob ] | [ regex ] ] ... ]
show running-config https
show running-config https [ [ name ] | [ glob ] | [ regex ] ] ... ]
options:
   all-properties
   non-default-properties
   one-line
   partition

Delete

delete https [ name ]

◆ Note
You cannot delete default monitors.

Description

You can use the https component to configure a custom monitor, or you can use the default HTTPS monitor that Local Traffic Manager provides. This type of monitor verifies the HTTPS service by attempting to receive specific content from a web page protected by Secure Socket Layer (SSL) security.

One of the pre-configured HTTPS monitors is named https_443, which performs a health check on a server using the IP address supplied by the pool member and port 443.

Examples

Creates a monitor named my_https that inherits properties from the default HTTPS monitor.

create https my_https defaults-from https

Displays the properties of all of the HTTPS monitors:

list https

Options

You can use these options with the https component:

◆ cert
   Specifies a fully-qualified path for a client certificate that the monitor sends to the target SSL server. The default value is none.
◆ cipherlist
   Specifies the list of ciphers for this monitor. The default list
   DEFAULT:+SHA:+3DES:+kEDH is located in the file
   base_monitors.conf.

◆ compatibility
   Specifies, when enabled, that the SSL options setting (in OpenSSL) is set
to ALL. The default value is enabled.

◆ defaults-from
   Specifies the name of the monitor from which you want your custom
   monitor to inherit settings. The default value is https.

◆ description
   User-defined description.

◆ destination
   Specifies the IP address and service port of the resource that is the
   destination of this monitor. The default value is *:*.
   Possible values are:
   • *:*  
     Specifies that the system marks a pool member up or down based on
     the response of the server at the IP address and port supplied by the
     pool member.
   • *:port
     Specifies that the system marks a pool member up or down based on
     the response of the server at the IP address supplied by the pool
     member and the port you specify.
   • <IP address>:<port>
     Specifies that the system marks a pool member up or down based on
     the response of the server at the IP address and port you specify.
   • <IP address>:<port> (with the transparent option enabled)
     Specifies that the system performs a health check on the server at the
     IP address and port you specify, routes the check through the IP
     address and port supplied by the pool member, and marks the pool
     member (the gateway) up or down accordingly.

◆ glob
   Displays the items that match the glob expression. For a description of
   glob expression syntax, see the glob man page.

◆ interval
   Specifies, in seconds, the frequency at which the system issues the
   monitor check when either the resource is down or the status of the
   resource is unknown. The default value is 5 seconds.

◆ key
   Specifies the RSA private key if the monitored target requires
   authentication. The key must be surrounded by quotation marks, for
   example: key "client.key". If you specify a key, you must also specify
   a value for the cert option. The default value is none.
◆ **manual-resume**  
   Specifies whether the system automatically changes the status of a resource to **up** at the next successful monitor check. The default value of the **manual-resume** option is **disabled**.

   If you set the **manual-resume** option to **enabled**, you must manually mark the resource as **up** before the system can use it for load balancing connections.

◆ **name**  
   Specifies a unique name for the component. This option is required for the commands **create**, **delete**, and **modify**.

◆ **partition**  
   Displays the administrative partition in which the component resides.

◆ **password**  
   Specifies the password if the monitored target requires authentication. The default value is **none**.

◆ **recv**  
   Specifies the text string that the monitor looks for in the returned resource. The default value is **none**.

   The most common receive expressions contain a text string that is included in an HTML file on your site. The text string can be regular text, HTML tags, or image names. If you do not specify a value for both the **send** and **recv** options, the monitor performs a simple service check and connect only.

◆ **recv-disable**  
   Specifies the text string that the monitor looks for in the returned resource. If the text string is matched in the returned resource, the corresponding node or pool member is marked **session disabled**. The default value is **none**.

   You specify a **recv-disable** string in the same way that you specify a **recv** string.

   If you specify a **recv-disable** string, you must also specify a **recv** string. You cannot specify a **recv-disable** string, if the **reverse** option is **enabled**.

◆ **regex**  
   Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. For a description of regular expression syntax, see the **regex** man page.

◆ **reverse**  
   Specifies whether the monitor operates in reverse mode. When the monitor is in reverse mode, a successful check marks the monitored object **down** instead of **up**. You can use the this mode only if you configure both the **send** and **recv** options.

   The default value is **disabled**. The **disabled** value specifies that the monitor does not operate in reverse mode. The **enabled** value specifies that the monitor operates in reverse mode.
itm monitor Module Components

◆ **send**
  Specifies the text string that the monitor sends to the target object. The default value is GET /, which retrieves a default HTML file for a web site.
  To retrieve a specific page from a web site, specify a fully-qualified path name, for example: GET /www/company/index.html. Since the string can have special characters, the system requires that the string be enclosed with single quotation marks.
  If this value is null, then a valid connection suffices to determine that the service is up. In this case, the system does not need the recv option and ignores the option even if not null.

◆ **time-until-up**
  Specifies the amount of time, in seconds, after the first successful response before a node is marked up. A value of 0 (zero) causes a node to be marked up immediately after a valid response is received from the node. The default value is 0 (zero).

◆ **timeout**
  Specifies the number of seconds the target has in which to respond to the monitor request. The default value is 16 seconds.
  If the target responds within the set time period, it is considered up. If the target does not respond within the set time period, it is considered down. Also, if the target responds with a RESET packet, the system immediately flags the target as down without waiting for the timeout interval to expire.

◆ **transparent**
  Specifies whether the monitor operates in transparent mode. Monitors in transparent mode can monitor pool members through firewalls. The default value is disabled.

◆ **up-interval**
  Specifies, in seconds, the frequency at which the system issues the monitor check when the resource is up. The default value is 0 (zero), which specifies that the system uses the value of the interval option whether the resource is up or down.
  **Important:** F5 Networks recommends that when you configure this option and the interval option, that the value that is greater be a multiple of the lesser value to allow for an even distribution of monitor checks among all monitors.

◆ **username**
  Specifies the user name if the monitored target requires authentication. The default value is none.

See also

create, delete, edit, glob, list, modify, regex, show, tmsh
**icmp**

Configures an Internet Control Message Protocol (ICMP) monitor.

**Module**

`ltm monitor`

**Syntax**

Configure the `icmp` component within the `ltm monitor` module using the following syntax.

**Create/Modify**

```
create icmp [name]
modify icmp [name]
   options:
       defaults-from [name]
       description [string]
       destination [ip address]
       interval [integer]
       manual-resume [enabled | disabled]
       time-until-up [integer]
       timeout [integer]
       transparent [enabled | disabled]
       up-interval [integer]
```

**Display**

```
list icmp
list icmp [ [name] | [glob] | [regex] ] ...
show running-config icmp
show running-config icmp [ [name] | [glob] | [regex] ] ...
   options:
       all-properties
       non-default-properties
       one-line
       partition
```
Delete

`delete icmp [name]`

**Note**

You cannot delete default monitors.

Description

You can use the `icmp` component to configure a custom monitor, or you can use the default ICMP monitor that Local Traffic Manager provides.

Examples

Creates a monitor named `my_icmp` that inherits properties from the default ICMP monitor.

`create icmp my_icmp defaults-from icmp`

Displays the properties of all of the ICMP monitors:

`list icmp`

Options

You can use these options with the `icmp` component:

- `defaults-from`
  Specifies the name of the monitor from which you want your custom monitor to inherit settings. The default value is `icmp`.

- `description`
  User-defined description.

- `destination`
  Specifies the IP address of the resource that is the destination of this monitor. The default value is `*`.
  Possible values are:
  - `*`
    Specifies that the system performs a health check on the IP address of the node.
  - `<IP address>`
    Specifies that the system performs a health check on the IP address that you specify and marks the associated node **up** or **down** as a result of the response.
  - `<IP address>` (with the `transparent` option enabled)
    Specifies that the system performs a health check on the IP address that you specify, routes the check through the IP address of the associated node, and marks the IP address of the associated node **up** or **down** accordingly.
◆ **glob**
Displays the items that match the **glob** expression. For a description of **glob** expression syntax, see the **glob** man page.

◆ **interval**
Specifies, in seconds, the frequency at which the system issues the monitor check when either the resource is **down** or the status of the resource is unknown. The default value is **5** seconds.

◆ **manual-resume**
Specifies whether the system automatically changes the status of a resource to **up** at the next successful monitor check. The default value of the **manual-resume** option is **disabled**.

If you set the **manual-resume** option to **enabled**, you must manually mark the resource as **up** before the system can use it for load balancing connections.

◆ **name**
Specifies a unique name for the component. This option is required for the commands **create**, **delete**, and **modify**.

◆ **partition**
Displays the administrative partition in which the component resides.

◆ **regex**
Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. For a description of regular expression syntax, see the **regex** man page.

◆ **time-until-up**
Specifies the amount of time, in seconds, after the first successful response before a node is marked **up**. A value of **0** (zero) causes a node to be marked **up** immediately after a valid response is received from the node. The default value is **0** (zero).

◆ **timeout**
Specifies the number of seconds the target has in which to respond to the monitor request. The default value is **16** seconds.

If the target responds within the set time period, it is considered **up**. If the target does not respond within the set time period, it is considered **down**. Also, if the target responds with a RESET packet, the system immediately flags the target as **down** without waiting for the timeout interval to expire.

◆ **transparent**
Specifies whether the monitor operates in transparent mode. Monitors in transparent mode can monitor pool members through firewalls. The default value is **disabled**.
◆ up-interval
   Specifies, in seconds, the frequency at which the system issues the monitor check when the resource is up. The default value is 0 (zero), which specifies that the system uses the value of the interval option whether the resource is up or down.

   Important: F5 Networks recommends that when you configure this option and the interval option, that the value that is greater be a multiple of the lesser value to allow for an even distribution of monitor checks among all monitors.

See also

create, delete, edit, glob, list, modify, regex, show, tmsh
imap

Configures an Internet Message Access Protocol (IMAP) monitor.

Module

ltm monitor

Syntax

Configure the imap component within the ltm monitor module using the following syntax.

Create/Modify

create imap [name]
modify imap [name]
options:
    debug [no | yes]
    defaults-from [name]
    description [string]
    destination [ip address][port]
    folder [ [name] | none]
    interval [integer]
    manual-resume [enabled | disabled]
    password [none | [password] ]
    time-until-up [integer]
    timeout [integer]
    up-interval [integer]
    username [ [name] | none]

edit imap [ [name] | [glob] | [regex] ] ... ]
options:
    all-properties
    non-default-properties

Display

list imap
list imap [ [name] | [glob] | [regex] ] ... ]
show running-config imap
show running-config imap [ [name] | [glob] | [regex] ] ... ]
options:
    all-properties
    non-default-properties
    one-line
    partition
Delete

```
delete imap [name]
```

◆ Note

You cannot delete default monitors.

Description

You can use the imap component to configure a custom monitor, or you can use the default IMAP monitor that Local Traffic Manager provides. This type of monitor verifies IMAP by attempting to open a specified mail folder on a server. This monitor is similar to the POP3 monitor.

Examples

Creates a monitor named my_imap that inherits properties from the default IMAP monitor:
```
create imap my_imap defaults-from imap
```

Displays the properties of all of the IMAP monitors:
```
list imap
```

Options

You can use these options with the imap component:

◆ debug
  Specifies whether the monitor sends error messages and additional information to a log file created and labeled specifically for this monitor. You can use the log information to help diagnose and troubleshoot unsuccessful health checks. The default value is no.
  
  The options are:
  
  * no
    Specifies that the system does not redirect error messages and additional information related to this monitor.
  
  * yes
    Specifies that the system redirects error messages and additional information to the
    `/var/log/<monitor_type>_<IP address>_<port>.log` file.

◆ defaults-from
  Specifies the name of the monitor from which you want your custom monitor to inherit settings. The default value is imap.

◆ description
  User-defined description.
- **destination**
  Specifies the IP address and service port of the resource that is the destination of this monitor. The default value is `*::*`. Possible values are:
  - `*::*`
    Specifies that the system marks a pool member **up** or **down** based on the response of the server at the IP address and port supplied by the pool member.
  - `*:port`
    Specifies that the system marks a pool member **up** or **down** based on the response of the server at the IP address supplied by the pool member and the port you specify.
  - `<IP address>:<port>`
    Specifies that the system marks a pool member **up** or **down** based on the response of the server at the IP address and port you specify.

- **folder**
  Specifies the name of the folder on the IMAP server that the monitor tries to open. The default value is **INBOX**.

- **glob**
  Displays the items that match the glob expression. For a description of glob expression syntax, see the glob man page.

- **interval**
  Specifies, in seconds, the frequency at which the system issues the monitor check when either the resource is **down** or the status of the resource is unknown. The default value is **10** seconds.

- **manual-resume**
  Specifies whether the system automatically changes the status of a resource to **up** at the next successful monitor check. The default value is disabled.
  If you set the **manual-resume** option to enabled, you must manually mark the resource as **up** before the system can use it for load balancing connections.

- **name**
  Specifies a unique name for the component. This option is required for the commands create, delete, and modify.

- **partition**
  Displays the administrative partition in which the component resides.

- **password**
  Specifies the password if the monitored target requires authentication. The default value is none.

- **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (`@[regular expression]`) to indicate that the identifier is a regular expression. For a description of regular expression syntax, see the regex man page.
◆ **time-until-up**
   Specifies the amount of time, in seconds, after the first successful response before a node is marked **up**. A value of 0 (zero) causes a node to be marked **up** immediately after a valid response is received from the node. The default value is 0 (zero).

◆ **timeout**
   Specifies the number of seconds the target has in which to respond to the monitor request. The default value is 31 seconds.

   If the target responds within the set time period, it is considered **up**. If the target does not respond within the set time period, it is considered **down**. Also, if the target responds with a RESET packet, the system immediately flags the target as **down** without waiting for the timeout interval to expire.

◆ **up-interval**
   Specifies, in seconds, the frequency at which the system issues the monitor check when the resource is **up**. The default value is 0 (zero), which specifies that the system uses the value of the **interval** option whether the resource is **up** or **down**.

   **Important:** F5 Networks recommends that when you configure this option and the **interval** option, that the value that is greater be a multiple of the lesser value to allow for an even distribution of monitor checks among all monitors.

◆ **username**
   Specifies the user name if the monitored target requires authentication. The default value is **none**.

**See also**

create, delete, edit, glob, list, modify, regex, show, tmsh
inband

Configures an Inband (passive) monitor.

Module

ltm monitor

Syntax

Configure the inband component within the ltm monitor module using the following syntax.

Create/Modify

create inband [name]
modify inband [name]
options:
  all
  defaults-from [name]
  description [string]
  failure-interval [integer]
  failures [integer]
  response-time [integer]
  retry-time [integer]
edit inband [ [ [name] | [glob] | [regex] ] ... ]
options:
  all-properties
  non-default-properties

Display

list inband
list inband [ [ [name] | [glob] | [regex] ] ... ]
show running-config inband
show running-config inband [ [ [name] | [glob] | [regex] ] ... ]
options:
  all-properties
  non-default-properties
  one-line
  partition
Delete

\[ \text{delete inband [name]} \]

\[ \text{Note} \]

You cannot delete default monitors.

Description

You can use the \text{inband} component to configure a custom monitor, or you can use the default Inband monitor that Local Traffic Manager provides. With this type of monitor the BIG-IP® system can perform passive monitoring as part of client requests.

Examples

Creates a monitor named \text{my_inband} that inherits properties from the default Inband monitor.

\[ \text{create inband my_inband defaults-from inband} \]

Displays the properties of all of the Inband monitors:

\[ \text{list inband} \]

Options

You can use these options with the \text{inband} component:

\[ \text{◆ defaults-from} \]

Specifies the name of the monitor from which you want your custom monitor to inherit settings. The default value is \text{inband}.

\[ \text{◆ description} \]

User-defined description.

\[ \text{◆ failure-interval} \]

Specifies an interval, in seconds. If the number of failures specified in the \text{failures} option occurs within this interval, the system marks the pool member as being unavailable. The default value is 30.

\[ \text{◆ failures} \]

Specifies the number of failures that the system allows to occur, within the time period specified in the \text{failure-interval} option, before marking a pool member unavailable. The default value is 3, which means that the system marks the pool member unavailable at the fourth failure. Specifying a value of 0 (zero) disables this option.

A \text{failure} can be either a failure to connect or a failure of the pool member to respond within the time specified in the \text{response-time} option.
◆ **glob**
   Displays the items that match the glob expression. For a description of glob expression syntax, see the glob man page.

◆ **name**
   Specifies a unique name for the component. This option is required for the commands create, delete, and modify.

◆ **partition**
   Displays the administrative partition within which the component resides.

◆ **regex**
   Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. For a description of regular expression syntax, see the regex man page.

◆ **response-time**
   Specifies an amount of time, in seconds. If the pool member does not respond with data after the specified amount of time has passed, the number of failures in this interval increments by 1. Specifying a value of 0 (zero) disables this option.

◆ **retry-time**
   Specifies the amount of time in seconds after the pool member has been marked unavailable before the system retries to connect to the pool member. Specifying a value of 0 (zero) disables this option.

### See also

create, delete, edit, glob, list, modify, regex, show, tmsh
ltm monitor Module Components

ldap


Module

ltm monitor

Syntax

Configure the ldap component within the ltm monitor module using the following syntax.

Create/Modify

create ldap [name]
modify ldap [name]
    options:
        base [none | [string] ]
        chase-referrals [no | yes]
        debug [no | yes]
        defaults-from [name]
        description [string]
        destination [ip address][port]
        filter [ [LDAP key] | none]
        interval [integer]
        mandatory-attributes [no | yes]
        manual-resume [enabled | disabled]
        password [none | [password] ]
        security [none | ssl | tls]
        time-until-up [integer]
        timeout [integer]
        up-interval [integer]
        username [ [name] | none]

edit ldap [ [ [name] | [glob] | [regex] ] ... ]
    options:
        all-properties
        non-default-properties

Display

list ldap
list ldap [ [ [name] | [glob] | [regex] ] ... ]
show running-config ldap
show running-config ldap [ [ name ] | [ glob ] | [ regex ] ] ... 

options:
  all-properties
  non-default-properties
  one-line
  partition

Delete

delete ldap [ name ]

◆ Note
You cannot delete default monitors.

Description

You can use the ldap component to configure a custom monitor, or you can use the default LDAP monitor that Local Traffic Manager provides. This type of monitor verifies the LDAP service by attempting to authenticate the specified user.

Examples

Creates a monitor named my_ldap that inherits properties from the default LDAP monitor.
create ldap my_ldap defaults-from ldap

Displays the properties of all of the LDAP monitors:
list ldap

Options

You can use these options with the ldap component:

◆ base
  Specifies the location in the LDAP tree from which the monitor starts the health check. A sample value is dc=bigip-test,dc=net. The default value is none.

◆ chase-referrals
  Specifies whether the monitor upon receipt of an LDAP referral entry chases that referral. The default value is yes.
◆ debug
Specifies whether the monitor sends error messages and additional information to a log file created and labeled specifically for this monitor. You can use the log information to help diagnose and troubleshoot unsuccessful health checks. The default value is no.
The options are:
  • no
    Specifies that the system does not redirect error messages and additional information related to this monitor.
  • yes
    Specifies that the system redirects error messages and additional information to the /var/log/<monitor_type>_<IP address>.<port>.log file.
◆ defaults-from
Specifies the name of the monitor from which you want your custom monitor to inherit settings. The default value is ldap.
◆ description
User-defined description.
◆ destination
Specifies the IP address and service port of the resource that is the destination of this monitor. The default value is *:*.
Possible values are:
  • *:*  
    Specifies that the system marks a pool member up or down based on the response of the server at the IP address and port supplied by the pool member.
  • *:port
    Specifies that the system marks a pool member up or down based on the response of the server at the IP address supplied by the pool member and the port you specify.
  • <IP address>:<port>
    Specifies that the system marks a pool member up or down based on the response of the server at the IP address and port you specify.
◆ filter
Specifies an LDAP key for which the monitor searches. A sample value is objectclass=*. The default value is none.
◆ glob
Displays the items that match the glob expression. For a description of glob expression syntax, see the glob man page.
◆ interval
Specifies, in seconds, the frequency at which the system issues the monitor check when either the resource is down or the status of the resource is unknown. The default value is 10 seconds.
◆ **mandatory-attributes**  
Specifies whether the target must include attributes in its response to be considered **up**. The default value is **no**.

The options are:

- **no**  
  Specifies that the system performs only a one-level search (based on the value of the **filter** option) and does not require that the target returns any attributes.

- **yes**  
  Specifies that the system performs a sub-tree search, and if the target returns no attributes, the target is considered down.

◆ **manual-resume**  
Specifies whether the system automatically changes the status of a resource to **up** at the next successful monitor check. The default value of the **manual-resume** option is **disabled**.

If you set the **manual-resume** option to **enabled**, you must manually mark the resource as **up** before the system can use it for load balancing connections.

◆ **name**  
Specifies a unique name for the component. This option is required.

◆ **partition**  
Displays the administrative partition in which the component resides.

◆ **password**  
Specifies the password if the monitored target requires authentication. The default value is **none**.

◆ **regex**  
Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. For a description of regular expression syntax, see the **regex** man page.

◆ **security**  
Specifies the secure communications protocol that the monitor uses to communicate with the target. The default value is **none**.

The options are:

- **none**  
  Specifies that the system does not use a security protocol for communications with the target.

- **ssl**  
  Specifies that the system uses the SSL protocol for communications with the target.

- **tls**  
  Specifies that the system uses the TLS protocol for communications with the target.
- **time-until-up**
  Specifies the amount of time, in seconds, after the first successful response before a node is marked **up**. A value of **0** (zero) causes a node to be marked **up** immediately after a valid response is received from the node. The default value is **0** (zero).

- **timeout**
  Specifies the number of seconds the target has in which to respond to the monitor request. The default value is **31** seconds.
  If the target responds within the set time period, it is considered **up**. If the target does not respond within the set time period, it is considered **down**. Also, if the target responds with a RESET packet, the system immediately flags the target as **down** without waiting for the timeout interval to expire.

- **up-interval**
  Specifies, in seconds, the frequency at which the system issues the monitor check when the resource is **up**. The default value is **0** (zero), which specifies that the system uses the value of the **interval** option whether the resource is **up** or **down**.

  **Important:** F5 Networks recommends that when you configure this option and the **interval** option, that the value that is greater be a multiple of the lesser value to allow for an even distribution of monitor checks among all monitors.

- **username**
  Specifies the user name if the monitored target requires authentication. The default value is **none**.

---

**See also**

create, delete, list, modify, show, tmsh
module-score

Configures a Module Score monitor that monitors the performance of a pool or node, rather than the health of the pool or node.

Module

ltm monitor

Syntax

Configure the module-score component within the ltm monitor module using the following syntax.

Create/Modify

create module-score [name]
modify module-score [name]
  options:
    debug [no | yes]
    defaults-from [name]
    description [string]
    interval [integer]
    pool [name]
    snmp-community [none | [string] ]
    snmp-ip-address [ [ip address] | none]
    snmp-port [port]
    snmp-version [string]
    time-until-up [integer]
    timeout [integer]
    up-interval [integer]
edit module-score [ [ [name] | [glob] | [regex] ] ... ]
  options:
    all-properties
    non-default-properties

Display

list module-score
list module-score [ [ [name] | [glob] | [regex] ] ... ]
show running-config module-score
show running-config module-score [ [ [name] | [glob] | [regex] ] ... ]
  options:
    all-properties
    non-default-properties
    one-line
    partition
Delete

```
delete module-score [name]
```

◆ Note

*You cannot delete default monitors.*

Description

You can use the `module-score` component to configure a custom monitor, or you can use the default Module Score monitor that Local Traffic Manager provides. This type of monitor enables Global Traffic Manager™ and Local Traffic Manager systems to load balance in a proportional manner to Local Traffic Manager virtual servers associated with the WebAccelerator™ system and Application Security Manager™. When you configure a Module Score type of monitor, the Local Traffic Manager system uses SNMP to pull the `gtm_score` values from the downstream virtual servers and set the dynamic ratios on the associated upstream Local Traffic Manager pool members or nodes.

More specifically, the Module Score monitor retrieves the `gtm_score` values from the virtual server and the `gtm_vs_score` values associated with the virtual server. Then, if a pool name is not specified, this monitor sets the dynamic ratio on the node that is associated with the virtual server.

The BIG-IP system uses the lowest non-zero value of the `gtm_vs_score` values to set the dynamic ratio. If all `gtm_vs_score` values are zero, then the `gtm_score` value is used to set the dynamic ratios. If you specify a pool name in the monitor definition, then the dynamic ratio is set on the pool member.

◆ Note

*If you want to distribute traffic to a cluster of WebAccelerator or Application Security Manager virtual servers, you must create a separate custom Module Score monitor for each back-end Local Traffic Manager system.*

Examples

Creates a monitor named `my_module-score` that inherits properties from the default module score monitor.

```
create module-score my_module-score defaults-from module_score
```

Displays the properties of all of the module score monitors:

```
list module-score
```
Options

You can use these options with the module-score component:

- **debug**
  Specifies whether the monitor sends error messages and additional information to a log file created and labeled specifically for this monitor. You can use the log information to help diagnose and troubleshoot unsuccessful health checks. The default value is **no**.

  The options are:
  - **no**
    Specifies that the system does not redirect error messages and additional information related to this monitor.
  - **yes**
    Specifies that the system redirects error messages and additional information to the `/var/log/<monitor_type>_<ip address>.<port>.log` file.

- **defaults-from**
  Specifies the name of the monitor from which you want the custom monitor to inherit settings. The default value is **module_score**.

- **description**
  User-defined description.

- **glob**
  Displays the items that match the glob expression. For a description of glob expression syntax, see the glob man page.

- **interval**
  Specifies, in seconds, the frequency at which the system issues the monitor check when either the resource is **down** or the status of the resource is unknown. The default value is 10 seconds.

- **name**
  Specifies a unique name for the component. option is required for the commands create, delete, and modify.

- **partition**
  Displays the administrative partition in which the component resides.

- **pool**
  Specifies a Local Traffic Manager pool name. Use this option if you want the system to set dynamic ratios on a pool member instead of on the associated node for the pool member. The default value is **none**.

- **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. For a description of regular expression syntax, see the regex man page.

- **snmp-community**
  Specifies the identifier for the SNMP community. The default value is **public**.

- **snmp-ip-address**
  Specifies the IP address of the SNMP server. The default value is **none**.
◆ **snmp-port**
   Specifies the port associated with the SNMP server. The default value is 161.

◆ **snmp-version**
   Specifies the SNMP version in use by the system. The default value is v2c.

◆ **time-until-up**
   Specifies the amount of time in seconds after the first successful response before a node is marked up. A value of 0 (zero) causes a node to be marked up immediately after a valid response is received from the node. The default value is 0 (zero).

◆ **timeout**
   Specifies the number of seconds the target has in which to respond to the monitor request. The default value is 30 seconds.

   If the target responds within the set time period, it is considered **up**. If the target does not respond within the set time period, it is considered **down**. Also, if the target responds with a RESET packet, the system immediately flags the target as **down** without waiting for the timeout interval to expire.

◆ **up-interval**
   Specifies, in seconds, the frequency at which the system issues the monitor check when the resource is **up**. The default value is 0 (zero), which specifies that the system uses the value of the **interval** option whether the resource is **up** or **down**.

   **Important:** F5 Networks recommends that when you configure this option and the **interval** option, that the value that is greater be a multiple of the lesser value to allow for an even distribution of monitor checks among all monitors.

**See also**

create, delete, edit, glob, list, modify, regex, show, tmsh
Chapter 31

mssql

Configures a Microsoft® Windows® Structured Query Language (MSSQL) monitor.

Module

ltm monitor

Syntax

Configure the mssql component within the ltm monitor module using the following syntax.

Create/Modify

create mssql [name]
modify mssql [name]

options:
  count [0 | 1]
database [ [name] | none]
d debug [no | yes]
defaults-from [name]
description [string]
destination [ip address][port]
interval [integer]
manual-resume [enabled | disabled]
password [none | [password] ]
recv [none | [string] ]
recv-column [none | [string] ]
recv-row [none | [string] ]
send [none | [string] ]
time-until-up [integer]
timeout [integer]
up-interval [integer]
username [ [name] | none]

edit mssql [ [ [name] | [glob] | [regex] ] ... ]

options:
  all-properties
  non-default-properties
Display

```
list mssql
list mssql [ [name] | [glob] | [regex] ] ...
show running-config mssql
show running-config mssql [ [name] | [glob] | [regex] ] ...
```

```
options:
  all-properties
  non-default-properties
  one-line
  partition
```

Delete

```
delete mssql [name]
```

◆ Note

*You cannot delete default monitors.*

Description

You can use the `mssql` component to configure a custom monitor, or you can use the default Microsoft Windows SQL monitor that Local Traffic Manager provides. This type of monitor verifies Microsoft Windows SQL-based services.

Examples

Creates a monitor named `my_mssql` that inherits properties from the default MSSQL monitor.

```
create mssql my_mssql defaults-from mssql
```

Displays the properties of all of the MSSQL monitors:

```
list mssql
```

Options

You can use these options with the `mssql` component:

◆ **count**

  Specifies the number of instances for which the system keeps a connection open. By default, when you assign instances of this monitor to a resource, the system keeps the connection to the database open. You can use this option to assign multiple instances to the database while reducing the overhead that multiple open connections can cause.
A value of 0 (zero), the default, keeps the connection open for all instances. A value of 1 opens a new connection for each instance. Any other positive value keeps the connection open for that many instances; for example, a value of 5 keeps the connection open for five instances of this monitor.

- **database**
  Specifies the name of the database with which the monitor attempts to communicate. The default value is **none**.

- **debug**
  Specifies whether the monitor sends error messages and additional information to a log file created and labeled specifically for this monitor. You can use the log information to help diagnose and troubleshoot unsuccessful health checks. The default value is **no**.
  The options are:
  - **no**
    Specifies that the system does not redirect error messages and additional information related to this monitor.
  - **yes**
    Specifies that the system redirects error messages and additional information to the `/var/log/<monitor_type>_<ip address>..<port>.log` file.

- **defaults-from**
  Specifies the name of the monitor from which you want your custom monitor to inherit settings. The default value is **mssql**.

- **description**
  User-defined description.

- **destination**
  Specifies the IP address and service port of the resource that is the destination of this monitor. The default value is ***:***.
  Possible values are:
  - ***:***
    Specifies that the system marks a pool member **up** or **down** based on the response of the server at the IP address and port supplied by the pool member.
  - ***:port**
    Specifies that the system marks a pool member **up** or **down** based on the response of the server at the IP address supplied by the pool member and the port you specify.
  - **<IP address>..<port>**
    Specifies that the system marks a pool member **up** or **down** based on the response of the server at the IP address and port you specify.

- **glob**
  Displays the items that match the **glob** expression. For a description of **glob** expression syntax, see the **glob** man page.
◆ **interval**  
Speifies, in seconds, the frequency at which the system issues the monitor check when either the resource is down or the status of the resource is unknown. The default value is 30 seconds.

◆ **manual-resume**  
Specifies whether the system automatically changes the status of a resource to up at the next successful monitor check. The default value of the manual-resume option is disabled.

If you set the manual-resume option to enabled, you must manually mark the resource as up before the system can use it for load balancing connections.

◆ **name**  
Specifies a unique name for the component. This option is required for the commands create, delete, and modify.

◆ **partition**  
Displays the administrative partition in which the component resides.

◆ **password**  
Specifies the password if the monitored target requires authentication. The default value is none.

◆ **recv**  
Specifies the text string that the monitor looks for in the returned resource. The default value is none.

The most common receive expressions contain a text string that is included in a field in your database. If you do not specify a value for both the send and recv options, the monitor performs a simple service check and connect only.

◆ **recv-column**  
Specifies the column in the database where the system expects the specified Receive String to be located. Specify this option only if you configure the send and recv options. The default value is none.

◆ **recv-row**  
Specifies the row in the database where the system expects the specified Receive String to be located. Specify this option only if you configure the send and recv options. The default value is none.

◆ **regex**  
Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. For a description of regular expression syntax, see the regex man page.

◆ **send**  
Specifies the SQL query that the monitor sends to the target database, for example: SELECT count(*) FROM mytable.

If this value is null, then a valid connection suffices to determine that the service is up. In this case, the system does not need the recv option and ignores the option even if not null.
◆ **time-until-up**
Specifies the amount of time in seconds after the first successful response before a node is marked up. A value of 0 (zero) causes a node to be marked up immediately after a valid response is received from the node. The default value is 0 (zero).

◆ **timeout**
Specifies the number of seconds the target has in which to respond to the monitor request. The default value is 91 seconds.
If the target responds within the set time period, it is considered up. If the target does not respond within the set time period, it is considered down. Also, if the target responds with a RESET packet, the system immediately flags the target as down without waiting for the timeout interval to expire.

◆ **up-interval**
Specifies, in seconds, the frequency at which the system issues the monitor check when the resource is up. The default value is 0 (zero), which specifies that the system uses the value of the interval option whether the resource is up or down.

*Important:* F5 Networks recommends that when you configure this option and the interval option, that the value that is greater be a multiple of the lesser value to allow for an even distribution of monitor checks among all monitors.

◆ **username**
Specifies the user name if the monitored target requires authentication. The default value is none.

**See also**
create, delete, edit, glob, list, modify, regex, show, tmsh
configures a MySQL® monitor.

module

ltm monitor

syntax

Configure the mysql component within the ltm monitor module using the following syntax.

create/modify

create mysql [name]
modify mysql [name]

options:
- count [0 | 1]
- database [ [name] | none]
- debug [no | yes]
- defaults-from [name]
- description [string]
- destination [ip address][port]
- interval [integer]
- manual-resume [enabled | disabled]
- password [none | [password] ]
- recv [none | [string] ]
- recv-column [none | [string] ]
- recv-row [none | [string] ]
- send [none | [string] ]
- time-until-up [integer]
- timeout [integer]
- up-interval [integer]
- username [ [name] | none]

edit mysql [ [ [name] | [glob] | [regex] ] ... ]

options:
- all-properties
- non-default-properties
Display

list mysql
list mysql [ [name] | [glob] | [regex] ] ...
show running-config mysql
show running-config mysql [ [name] | [glob] | [regex] ] ...
options:
  all-properties
  non-default-properties
  one-line
  partition

Delete

delete mysql [name]

◆ Note

You cannot delete default monitors.

Description

You can use the mysql component to configure a custom monitor, or you can use the default MySQL monitor that Local Traffic Manager provides. This type of monitor verifies MySQL-based services.

Examples

Creates a monitor named my_mysql that inherits properties from the default MySQL monitor.

create mysql my_mysql defaults-from mysql

Displays the properties of all of the MySQL monitors:

list mysql

Options

You can use these options with the mysql component:

◆ count
  Specifies the number of instances for which the system keeps a connection open. By default, when you assign instances of this monitor to a resource, the system keeps the connection to the database open. You can use this option to assign multiple instances to the database while reducing the overhead that multiple open connections can cause.
A value of 0 (zero), the default, keeps the connection open for all instances. A value of 1 opens a new connection for each instance. Any other positive value keeps the connection open for that many instances; for example, a value of 5 keeps the connection open for five instances of this monitor.

- **database**
  Specifies the name of the database with which the monitor attempts to communicate. The default value is **none**.

- **debug**
  Specifies whether the monitor sends error messages and additional information to a log file created and labeled specifically for this monitor. You can use the log information to help diagnose and troubleshoot unsuccessful health checks. The default value is **no**.

  The options are:
  - **no**
    Specifies that the system does not redirect error messages and additional information related to this monitor.
  - **yes**
    Specifies that the system redirects error messages and additional information to the
    
    /var/log/<monitor_type>_<ip address>.<port>.log

  file.

- **defaults-from**
  Specifies the name of the monitor from which you want your custom monitor to inherit settings. The default value is **mssql**.

- **description**
  User-defined description.

- **destination**
  Specifies the IP address and service port of the resource that is the destination of this monitor. The default value is **:*:***.

  Possible values are:
  - **:*:***
    Specifies that the system marks a pool member **up or down** based on the response of the server at the IP address and port supplied by the pool member.
  - **:*:port**
    Specifies that the system marks a pool member **up or down** based on the response of the server at the IP address supplied by the pool member and the port you specify.
  - **<IP address>:<port>**
    Specifies that the system marks a pool member **up or down** based on the response of the server at the IP address and port you specify.

- **glob**
  Displays the items that match the **glob** expression. For a description of **glob** expression syntax, see the **glob** man page.
◆ interval
Specifies, in seconds, the frequency at which the system issues the monitor check when either the resource is down or the status of the resource is unknown. The default value is 30 seconds.

◆ manual-resume
Specifies whether the system automatically changes the status of a resource to up at the next successful monitor check. The default value of the manual-resume option is disabled.
If you set the manual-resume option to enabled, you must manually mark the resource as up before the system can use it for load balancing connections.

◆ name
Specifies a unique name for the component. This option is required for the commands create, delete, and modify.

◆ partition
Displays the administrative partition in which the component resides.

◆ password
Specifies the password if the monitored target requires authentication. The default value is none.

◆ recv
Specifies the text string that the monitor looks for in the returned resource. The default value is none.
The most common receive expressions contain a text string that is included in a field in your database. If you do not specify a value for both the send and recv options, the monitor performs a simple service check and connect only.

◆ recv-column
Specifies the column in the database where the system expects the specified Receive String to be located. Specify this option only if you configure the send and recv options. The default value is none.

◆ recv-row
Specifies the row in the database where the system expects the specified Receive String to be located. Specify this option only if you configure the send and recv options. The default value is none.

◆ regex
Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. For a description of regular expression syntax, see the regex man page.

◆ send
Specifies the SQL query that the monitor sends to the target database, for example: SELECT count(*) FROM mytable.
If this value is null, then a valid connection suffices to determine that the service is up. In this case, the system does not need the recv option and ignores the option even if not null.
◆ **time-until-up**
   Specifies the amount of time in seconds after the first successful response before a node is marked up. A value of 0 (zero) causes a node to be marked up immediately after a valid response is received from the node. The default value is 0 (zero).

◆ **timeout**
   Specifies the number of seconds the target has in which to respond to the monitor request. The default value is 91 seconds.

   If the target responds within the set time period, it is considered **up**. If the target does not respond within the set time period, it is considered **down**. Also, if the target responds with a RESET packet, the system immediately flags the target as **down** without waiting for the timeout interval to expire.

◆ **up-interval**
   Specifies, in seconds, the frequency at which the system issues the monitor check when the resource is **up**. The default value is 0 (zero), which specifies that the system uses the value of the interval option whether the resource is **up** or **down**.

   **Important:** F5 Networks recommends that when you configure this option and the interval option, that the value that is greater be a multiple of the lesser value to allow for an even distribution of monitor checks among all monitors.

◆ **username**
   Specifies the user name if the monitored target requires authentication. The default value is **none**.

**See also**

*create, delete, edit, glob, list, modify, regex, show, tmsh*
nntp

Configures a Network News Transfer Protocol (NNTP) monitor.

Module

ltm monitor

Syntax

Configure the nntp component within the ltm monitor module using the following syntax.

Create/Modify

create nntp [name]
modify nntp [name]
options:
dialog [no | yes]
defaults-from [name]
description [string]
destination [ip address][port]
interval [integer]
manual-resume [enabled | disabled]
newsgroup [ [name] | none]
password [none | [string] ]
time-until-up [integer]
timeout [integer]
up-interval [integer]
username [ [name] | none]
edit nntp [ [ [name] | [glob] | [regex] ] ... ]
options:
all-properties
non-default-properties

Display

list nntp
list nntp [ [ [name] | [glob] | [regex] ] ... ]
show running-config nntp
show running-config nntp [ [ [name] | [glob] | [regex] ] ... ]
options:
all-properties
non-default-properties
Delete

delete nntp [name]

◆ Note

You cannot delete default monitors.

Description

You can use the nntp component to configure a custom monitor, or you can use the default NNTP monitor that Local Traffic Manager provides. This type of monitor verifies the Usenet News protocol service by attempting to retrieve a newsgroup identification string from the server.

Examples

Creates a monitor named my_nntp that inherits properties from the default NNTP monitor.

create nntp my_nntp defaults-from nntp

Displays the properties of all of the NNTP monitors:

list nntp

Options

You can use these options with the nntp component:

◆ debug

Specifies whether the monitor sends error messages and additional information to a log file created and labeled specifically for this monitor. You can use the log information to help diagnose and troubleshoot unsuccessful health checks. The default value is no.

The options are:

• no

  Specifies that the system does not redirect error messages and additional information related to this monitor.

• yes

  Specifies that the system redirects error messages and additional information to the /var/log/<monitor_type>_<ip address>.<port>.log file.

◆ defaults-from

Specifies the name of the monitor from which you want your custom monitor to inherit settings. The default value is nntp.
◆ **description**
User-defined description.

◆ **destination**
Specifies the IP address and service port of the resource that is the destination of this monitor. The default value is `*::*`.

Possible values are:
- `*::*`
  Specifies that the system marks a pool member **up** or **down** based on the response of the server at the IP address and port supplied by the pool member.
- `*:port`
  Specifies that the system marks a pool member **up** or **down** based on the response of the server at the IP address supplied by the pool member and the port you specify.
- `<IP address>:<port>`
  Specifies that the system marks a pool member **up** or **down** based on the response of the server at the IP address and port you specify.

◆ **glob**
Displays the items that match the **glob** expression. For a description of **glob** expression syntax, see the **glob** man page.

◆ **interval**
Specifies, in seconds, the frequency at which the system issues the monitor check when either the resource is **down** or the status of the resource is unknown. The default value is 5 seconds.

◆ **manual-resume**
Specifies whether the system automatically changes the status of a resource to **up** at the next successful monitor check. The default value of the **manual-resume** option is **disabled**.

If you set the **manual-resume** option to **enabled**, you must manually mark the resource as **up** before the system can use it for load balancing connections.

◆ **name**
Specifies a unique name for the component. This option is required for the commands **create**, **delete**, and **modify**.

◆ **newsgroup**
Specifies the name of the newsgroup that you are monitoring, for example **alt.car.mercedes**. The default value is **none**.

◆ **partition**
Displays the administrative partition in which the component resides.

◆ **password**
Specifies the password if the monitored target requires authentication. The default value is **none**.

◆ **regex**
Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. For a description of regular expression syntax, see the **regex** man page.
◆ **time-until-up**
   Specifies the amount of time in seconds after the first successful response before a node is marked up. A value of 0 (zero) causes a node to be marked up immediately after a valid response is received from the node. The default value is 0 (zero).

◆ **timeout**
   Specifies the number of seconds the target has in which to respond to the monitor request. The default value is 16 seconds.

   If the target responds within the set time period, it is considered up. If the target does not respond within the set time period, it is considered down. Also, if the target responds with a RESET packet, the system immediately flags the target as down without waiting for the timeout interval to expire.

◆ **up-interval**
   Specifies, in seconds, the frequency at which the system issues the monitor check when the resource is up. The default value is 0 (zero), which specifies that the system uses the value of the interval option whether the resource is up or down.

   **Important:** F5 Networks recommends that when you configure this option and the interval option, that the value that is greater be a multiple of the lesser value to allow for an even distribution of monitor checks among all monitors.

◆ **username**
   Specifies the user name if the monitored target requires authentication. The default value is none.

---

**See also**

create, delete, edit, glob, list, modify, regex, show, tmsh
oracle

Configures an Oracle® monitor.

Module

ltm monitor

Syntax

Configure the oracle component within the ltm monitor module using the following syntax.

Create/Modify

create oracle [name]
m modify oracle [name]
options:
count [0 | 1]
database [ [name] | none]
d debug [no | yes]
defaults-from [name]
description [string]
destination [ip address][port]
d interval [integer]
d manual-resume [enabled | disabled]
password [none | [password] ]
recv [none | [string] ]
recv-column [none | [string] ]
recv-row [none | [string] ]
send [none | [string] ]
time-until-up [integer]
t timeout [integer]
up-interval [integer]
username [ [name] | none]
e dit oracle [ [ [name] | [glob] | [regex] ] ... ]
options:
all-properties
non-default-properties
Display

list oracle
list oracle [ [name] | [glob] | [regex] ] ... ]
show running-config oracle
show running-config oracle [ [name] | [glob] | [regex] ] ... ]

options:
  all-properties
  non-default-properties
  one-line
  partition

Delete

delete oracle [name]

◆ Note

You cannot delete default monitors.

Description

You can use the oracle component to configure a custom monitor, or you can use the default Oracle monitor that Local Traffic Manager provides. This type of monitor verifies Oracle database services.

Examples

Creates a monitor named my_oracle that inherits properties from the default Oracle monitor.

create oracle my_oracle defaults-from oracle

Displays the properties of all of the Oracle monitors:

list oracle

Options

You can use these options with the oracle component:

◆ count
  Specifies the number of instances for which the system keeps a connection open. By default, when you assign instances of this monitor to a resource, the system keeps the connection to the database open. You can use this option to assign multiple instances to the database while reducing the overhead that multiple open connections can cause.
A value of 0 (zero), the default, keeps the connection open for all instances. A value of 1 opens a new connection for each instance. Any other positive value keeps the connection open for that many instances; for example, a value of 5 keeps the connection open for five instances of this monitor.

◆ **database**

  Specifies the name of the database with which the monitor attempts to communicate. The default value is **none**.

◆ **debug**

  Specifies whether the monitor sends error messages and additional information to a log file created and labeled specifically for this monitor. You can use the log information to help diagnose and troubleshoot unsuccessful health checks. The default value is **no**.

  The options are:

  • **no**

    Specifies that the system does not redirect error messages and additional information related to this monitor.

  • **yes**

    Specifies that the system redirects error messages and additional information to the

    `/var/log/<monitor_type>_<ip address>.<port>.log`

    file.

◆ **defaults-from**

  Specifies the name of the monitor from which you want your custom monitor to inherit settings. The default value is **oracle**.

◆ **description**

  User-defined description.

◆ **destination**

  Specifies the IP address and service port of the resource that is the destination of this monitor. The default value is ***:***.

  Possible values are:

  • ***:***

    Specifies that the system marks a pool member **up** or **down** based on the response of the server at the IP address and port supplied by the pool member.

  • ***:<port>**

    Specifies that the system marks a pool member **up** or **down** based on the response of the server at the IP address supplied by the pool member and the port you specify.

  • **<IP address>:<port>**

    Specifies that the system marks a pool member **up** or **down** based on the response of the server at the IP address and port you specify.

◆ **glob**

  Displays the items that match the **glob** expression. For a description of **glob** expression syntax, see the **glob** man page.
◆ **interval**
   Specifies, in seconds, the frequency at which the system issues the monitor check when either the resource is **down** or the status of the resource is unknown. The default value is 30 seconds.

◆ **manual-resume**
   Specifies whether the system automatically changes the status of a resource to **up** at the next successful monitor check. The default value of the **manual-resume** option is **disabled**.
   If you set the **manual-resume** option to **enabled**, you must manually mark the resource as **up** before the system can use it for load balancing connections.

◆ **name**
   Specifies a unique name for the component. This option is required for the commands create, delete, and modify.

◆ **partition**
   Displays the administrative partition in which the component resides.

◆ **password**
   Specifies the password if the monitored target requires authentication. The default value is **none**.

◆ **recv**
   Specifies the text string that the monitor looks for in the returned resource. The default value is **none**.
   The most common receive expressions contain a text string that is included in a field in your database. If you do not specify a value for both the **send** and **recv** options, the monitor performs a simple service check and connect only.

◆ **recv-column**
   Specifies the column in the database where the system expects the specified Receive String to be located. Specify this option only if you configure the **send** and **recv** options. The default value is **none**.

◆ **recv-row**
   Specifies the row in the database where the system expects the specified Receive String to be located. Specify this option only if you configure the **send** and **recv** options. The default value is **none**.

◆ **regex**
   Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. For a description of regular expression syntax, see the **regex** man page.

◆ **send**
   Specifies the SQL query that the monitor sends to the target database, for example: **SELECT count(*) FROM mytable**.
   If this value is null, then a valid connection suffices to determine that the service is **up**. In this case, the system does not need the **recv** option and ignores the option even if not null.
◆ time-until-up
   Specifies the amount of time in seconds after the first successful response before a node is marked up. A value of 0 (zero) causes a node to be marked up immediately after a valid response is received from the node. The default value is 0 (zero).

◆ timeout
   Specifies the number of seconds the target has in which to respond to the monitor request. The default value is 91 seconds.

   If the target responds within the set time period, it is considered up. If the target does not respond within the set time period, it is considered down. Also, if the target responds with a RESET packet, the system immediately flags the target as down without waiting for the timeout interval to expire.

◆ up-interval
   Specifies, in seconds, the frequency at which the system issues the monitor check when the resource is up. The default value is 0 (zero), which specifies that the system uses the value of the interval option whether the resource is up or down.

   Important: F5 Networks recommends that when you configure this option and the interval option, that the value that is greater be a multiple of the lesser value to allow for an even distribution of monitor checks among all monitors.

◆ username
   Specifies the user name if the monitored target requires authentication. The default value is none.

See also

create, delete, edit, glob, list, modify, regex, show, tmsh
**pop3**

Configures a Post Office Protocol version 3 (POP3) monitor.

**Module**

ltm monitor

**Syntax**

Configure the `pop3` component within the `ltm monitor` module using the following syntax.

**Create/Modify**

```
create pop3 [name]
modify pop3 [name]
options:
  debug [no | yes]
  defaults-from [name]
  description [string]
  destination [ip address][port]
  interval [integer]
  manual-resume [enabled | disabled]
  password [none | [password] ]
  time-until-up [integer]
  timeout [integer]
  up-interval [integer]
  username [ [name] | none]
edit pop3 [ [ [name] | [glob] | [regex] ] ... ]
options:
  all-properties
  non-default-properties
```

**Display**

```
list pop3
list pop3 [ [ name ] [ glob ] [ regex ] ] ... 
show running-configuration pop3
show running-configuration pop3 [ [ name ] [ glob ] [ regex ] ] ... 
options:
  all-properties
  non-default-properties
  one-line
  partition
```
Delete

delete pop3 [name]

◆ Note

You cannot delete default monitors.

Description

You can use the pop3 component to configure a custom monitor, or you can use the default POP3 monitor that Local Traffic Manager provides. This type of monitor verifies the POP3 service by attempting to connect to a pool, pool member, or virtual server, logging on as the specified user, and logging off.

Examples

Creates a monitor named my_pop3 that inherits properties from the default POP3 monitor.
create pop3 my_pop3 defaults-from pop3

Displays the properties of all of the POP3 monitors:
list pop3

Options

You can use these options with the pop3 component:

◆ debug
  Specifies whether the monitor sends error messages and additional information to a log file created and labeled specifically for this monitor. You can use the log information to help diagnose and troubleshoot unsuccessful health checks. The default value is no.

  The options are:
  • no
    Specifies that the system does not redirect error messages and additional information related to this monitor.
  • yes
    Specifies that the system redirects error messages and additional information to the
    /var/log/<monitor_type>_<ip address>_<port>.log file.

◆ defaults-from
  Specifies the name of the monitor from which you want your custom monitor to inherit settings. The default value is pop3.

◆ description
  User-defined description.
◆ **destination**
Spectifies the IP address and service port of the resource that is the
destination of this monitor. The default value is `*:*
Possible values are:
- `*:*`
  Specifies that the system marks a pool member **up** or **down** based on
  the response of the server at the IP address and port supplied by the
  pool member.
- `*:port`
  Specifies that the system marks a pool member **up** or **down** based on
  the response of the server at the IP address supplied by the pool
  member and the port you specify.
- `<IP address>:<port>`
  Specifies that the system marks a pool member **up** or **down** based on
  the response of the server at the IP address and port you specify.

◆ **glob**
Displays the items that match the **glob** expression. For a description of
**glob** expression syntax, see the **glob** man page.

◆ **interval**
Specifies, in seconds, the frequency at which the system issues the
monitor check when either the resource is **down** or the status of the
resource is unknown. The default value is 5 seconds.

◆ **manual-resume**
Specifies whether the system automatically changes the status of a
resource to **up** at the next successful monitor check. The default value of
the **manual-resume** option is disabled.
If you set the **manual-resume** option to enabled, you must manually
mark the resource as **up** before the system can use it for load balancing
connections.

◆ **name**
Specifies a unique name for the component. This option is required for
the commands **create**, **delete**, and **modify**.

◆ **partition**
Displays the administrative partition in which the component resides.

◆ **password**
Specifies the password if the monitored target requires authentication.
The default value is **none**.

◆ **regex**
Displays the items that match the regular expression. The regular
expression must be preceded by an at sign (@[regular expression]) to
indicate that the identifier is a regular expression. For a description of
regular expression syntax, see the **regex** man page.

◆ **time-until-up**
Specifies the amount of time in seconds after the first successful response
before a node is marked up. A value of 0 (zero) causes a node to be
marked up immediately after a valid response is received from the node.
The default value is 0 (zero).
◆ **timeout**
   Specifies the number of seconds the target has in which to respond to the monitor request. The default value is 16 seconds.
   If the target responds within the set time period, it is considered **up**. If the target does not respond within the set time period, it is considered **down**. Also, if the target responds with a RESET packet, the system immediately flags the target as **down** without waiting for the timeout interval to expire.

◆ **up-interval**
   Specifies, in seconds, the frequency at which the system issues the monitor check when the resource is **up**. The default value is 0 (zero), which specifies that the system uses the value of the **interval** option whether the resource is **up** or **down**.
   **Important:** F5 Networks recommends that when you configure this option and the **interval** option, that the value that is greater be a multiple of the lesser value to allow for an even distribution of monitor checks among all monitors.

◆ **username**
   Specifies the user name if the monitored target requires authentication. The default value is **none**.

**See also**

create, delete, edit, glob, list, modify, regex, show, tmsh
postgresql

Configures a PostgreSQL® monitor.

Module

ltm monitor

Syntax

Configure the postgresql component within the ltm monitor module using the following syntax.

Create/Modify

create postgresql [name]
modify postgresql [name]

options:
  count [0 | 1]
  database [ [name] | none]
  debug [no | yes]
  defaults-from [name]
  description [string]
  destination [ip address][port]
  ignore-down-response [enabled | disabled]
  interval [integer]
  password [none | [password] ]
  probe-timeout [integer]
  recv [none | [string] ]
  recv-column [none | [string] ]
  recv-row [none | [string] ]
  send [none | [string] ]
  timeout [integer]
  username [ [name] | none]

edit postgresql [ [name] | [glob] | [regex] ] ... 

options:
  all-properties
  non-default properties
Display

list postgresql
list postgresql [ [name] | [glob] | [regex] ] ... ]
show running-config postgresql
show running-config postgresql [ [name] | [glob] | [regex] ] ... ]
  options:
    all-properties
    non-default-properties
    one-line
    partition

Delete

delete postgresql [name]

◆ Note
You cannot delete default monitors.

Description

You can use the postgresql component to configure a custom monitor, or you can use the default PostgreSQL monitor that the Global Traffic Manager provides. This type of monitor verifies Microsoft Windows SQL-based services.

Examples

Creates a monitor named my_postgresql that inherits properties from the default PostgreSQL monitor:
create postgresql my_postgresql defaults-from postgresql

Displays the properties of all of the PostgreSQL monitors:
list postgresql

Options

You can use these options with the postgresql component:

◆ count
  Specifies the number of instances for which the system keeps a connection open. By default, when you assign instances of this monitor to a resource, the system keeps the connection to the database open. With this option you can assign multiple instances to the database while reducing the overhead that multiple open connections can cause.
A value of 0 (zero), the default, keeps the connection open for all instances. A value of 1 opens a new connection for each instance. Any other positive value keeps the connection open for that many instances; for example, a value of 5 keeps the connection open for five instances of this monitor.

- **database**
  Specifies the name of the database with which the monitor attempts to communicate. The default value is none.

- **debug**
  Specifies whether the monitor sends error messages and additional information to a log file created and labeled specifically for this monitor. You can use the log information to help diagnose and troubleshoot unsuccessful health checks. The default value is no.

  The options are:
  - no
    Specifies that the system does not redirect error messages and additional information related to this monitor.
  - yes
    Specifies that the system redirects error messages and additional information to the /var/log/<monitor_type>_<ip address>_<port>.log file.

- **defaults-from**
  Specifies the name of the monitor from which you want your custom monitor to inherit settings. The default value is mssql.

- **description**
  User-defined description.

- **destination**
  Specifies the IP address and service port of the resource that is the destination of this monitor. The default value is *:*.*.

  Possible values are:
  - *:*.*
    Specifies that the system marks a pool member up or down based on the response of the server at the IP address and port supplied by the pool member.
  - *:port
    Specifies that the system marks a pool member up or down based on the response of the server at the IP address supplied by the pool member and the port you specify.
  - <IP address>:<port>
    Specifies that the system marks a pool member up or down based on the response of the server at the IP address and port you specify.

- **glob**
  Displays the items that match the glob expression. For a description of glob expression syntax, see the glob man page.

- **ignore-down-response**
  Specifies whether the monitor ignores a down response from the system it is monitoring. The default value is disabled.
◆ **interval**
   Specifies the frequency at which the system issues the monitor check. The default value is 30 seconds.

◆ **name**
   Specifies a unique name for the component. This option is required for the commands create, delete, and modify.

◆ **partition**
   Displays the administrative partition in which the component resides.

◆ **password**
   Specifies the password if the monitored target requires authentication. The default value is none.

◆ **probe-timeout**
   Specifies the number of seconds after which the BIG-IP system times out the probe request to the BIG-IP system. The default value is 5 seconds.

◆ **recv**
   Specifies the text string that the monitor looks for in the returned resource. The default value is none.
   The most common receive expressions contain a text string that is included in a field in your database. If you do not specify a value for both the send and recv options, the monitor performs only a simple service check and connect.

◆ **recv-column**
   Specifies the column in the database where the system expects the specified Receive String to be located. Specify this option only if you configure the send and recv options. The default value is none.

◆ **recv-row**
   Specifies the row in the database where the system expects the specified Receive String to be located. Specify this option only if you configure the send and recv options. The default value is none.

◆ **regex**
   Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. For a description of regular expression syntax, see the regex man page.

◆ **send**
   Specifies the SQL query that the monitor sends to the target database, for example: SELECT count(*) FROM mytable.
   If this value is null, then a valid connection suffices to determine that the service is up. In this case, the system does not need the recv option and ignores the option even if not null.
◆ **timeout**
   Specifies the number of seconds the target has in which to respond to the monitor request. The default value is **91** seconds.
   
   If the target responds within the set time period, it is considered **up**. If the target does not respond within the set time period, it is considered **down**.
   
   Also, if the target responds with a RESET packet, the system immediately flags the target as **down** without waiting for the timeout interval to expire.

◆ **username**
   Specifies the user name if the monitored target requires authentication. The default value is **none**.

See also

`create, delete, edit, glob, gtm pool, list, modify, regex show, tmsh`
radius

Configures a Remote Access Dial-in User Service (RADIUS) monitor.

Module

ltm monitor

Syntax

Configure the radius component within the ltm monitor module using the following syntax.

Create/Modify

create radius [name]
modify radius [name]
options:
  debug [no | yes]
  defaults-from [name]
  description [string]
  destination [ip address][port]
  interval [integer]
  manual-resume [enabled | disabled]
  nas-ip-address [ [ip address] | none]
  password [none | [password] ]
  secret [none | [secret] ]
  time-until-up [integer]
  timeout [integer]
  up-interval [integer]
  username [ [name] | none]
edit radius [ [ [name] | [glob] | [regex] ] ... ]
  options:
    all-properties
    non-default-properties

Display

list radius
list radius [ [ [name] | [glob] | [regex] ] ... ]
show running-config radius
show running-config radius [ [ [name] | [glob] | [regex] ] ... ]
  options:
    all-properties
Delete

delete radius [name]

◆ Note

You cannot delete default monitors.

Description

You can use the `radius` component to configure a custom monitor, or you can use the default RADIUS monitor that Local Traffic Manager provides. This type of monitor verifies the RADIUS service by attempting to authenticate the specified user.

Examples

Creates a monitor named `my_radius` that inherits properties from the default RADIUS monitor.

`create radius my_radius defaults-from radius`

Displays the properties of all of the RADIUS monitors:

`list radius`

Options

You can use these options with the `radius` component:

◆ `debug`

Specifies whether the monitor sends error messages and additional information to a log file created and labeled specifically for this monitor. You can use the log information to help diagnose and troubleshoot unsuccessful health checks. The default value is `no`.

The options are:

• `no`

  Specifies that the system does not redirect error messages and additional information related to this monitor.

• `yes`

  Specifies that the system redirects error messages and additional information to the

  `/var/log/<monitor_type>_<ip address>_<port>.log` file.
◆ defaults-from
Specifies the name of the monitor from which you want your custom monitor to inherit settings. The default value is radius.

◆ description
User-defined description.

◆ destination
Specifies the IP address and service port of the resource that is the destination of this monitor. The default value is *:*.
Possible values are:
- *:*  
  Specifies that the system marks a pool member up or down based on the response of the server at the IP address and port supplied by the pool member.
- *:port  
  Specifies that the system marks a pool member up or down based on the response of the server at the IP address supplied by the pool member and the port you specify.
- <IP address>:<port>  
  Specifies that the system marks a pool member up or down based on the response of the server at the IP address and port you specify.

◆ glob
Displays the items that match the glob expression. For a description of glob expression syntax, see the glob man page.

◆ interval
Specifies, in seconds, the frequency at which the system issues the monitor check when either the resource is down or the status of the resource is unknown. The default value is 10 seconds.

◆ manual-resume
Specifies whether the system automatically changes the status of a resource to up at the next successful monitor check. The default value of the manual-resume option is disabled.
If you set the manual-resume option to enabled, you must manually mark the resource as up before the system can use it for load balancing connections.

◆ name
Specifies a unique name for the component. This option is required for the commands create, delete, and modify.

◆ nas-ip-address
Specifies the network access server IP address that the system uses to identify itself to the RADIUS server. With this option, multiple BIG-IP systems can appear as a single network access device to the RADIUS server. The default value is none.

◆ partition
Displays the administrative partition in which the component resides.

◆ password
Specifies the password if the monitored target requires authentication. The default value is none.
◆ **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. For a description of regular expression syntax, see the `regex` man page.

◆ **secret**
  Specifies the secret the monitor must use when contacting the resource. The default value is *none*.

◆ **time-until-up**
  Specifies the amount of time in seconds after the first successful response before a node is marked up. A value of 0 (zero) causes a node to be marked up immediately after a valid response is received from the node. The default value is 0 (zero).

◆ **timeout**
  Specifies the number of seconds the target has in which to respond to the monitor request. The default value is 31 seconds.

  If the target responds within the set time period, it is considered *up*. If the target does not respond within the set time period, it is considered *down*. Also, if the target responds with a RESET packet, the system immediately flags the target as *down* without waiting for the timeout interval to expire.

◆ **up-interval**
  Specifies, in seconds, the frequency at which the system issues the monitor check when the resource is *up*. The default value is 0 (zero), which specifies that the system uses the value of the `interval` option whether the resource is *up* or *down*.

  **Important:** F5 Networks recommends that when you configure this option and the `interval` option, that the value that is greater be a multiple of the lesser value to allow for an even distribution of monitor checks among all monitors.

◆ **username**
  Specifies the user name if the monitored target requires authentication. The default value is *none*.

---

**See also**

`create`, `delete`, `edit`, `glob`, `list`, `modify`, `regex`, `show`, `tmsh`
radius-accounting

Configures a Remote Access Dial-in User Service (RADIUS) accounting monitor for the BIG-IP Local Traffic Manager.

Module

ltm monitor

Syntax

Configure the radius-accounting component within the ltm monitor module using the following syntax.

Create/Modify

create radius-accounting [name]
modify radius-accounting [name]
  options:
    debug [no | yes]
    defaults-from [ [name] | none]
    destination [ip address]
    interval [integer]
    manual-resume [disabled | enabled]
    nas-ip-address [ip address]
    secret [string]
    time-until-up [integer]
    timeout [integer]
    up-interval [integer]
    username [none | [string]]

edit radius-accounting [ [ [name] | [glob] | [regex] ] ... ]
  options:
    all-properties
    non-default-properties

Display

list radius-accounting
list radius-accounting [ [ [name] | [glob] | [regex] ] ... ]
show running-config radius-accounting
show running-config radius-accounting [ [ [name] | [glob] | [regex] ] ... ]
  options:
    all-properties
    non-default-properties
    one-line
    partition
Delete

```
delete radius-accounting [name]
```

◆ **Note**

*You cannot delete default monitors.*

Description

You can use the `radius-accounting` component to configure a custom monitor, or you can use the default RADIUS accounting monitor that Local Traffic Manager provides.

Examples

Creates a monitor named `my_radius_acct` that inherits properties from the default RADIUS accounting monitor.

```
create radius my_radius_acct defaults-from radius_accounting
```

Displays the properties of all of the RADIUS accounting monitors:

```
list radius-accounting
```

Options

You can use these options with the `radius` component:

◆ **debug**

  Specifies whether the monitor sends error messages and additional information to a log file created and labeled specifically for this monitor. You can use the log information to help diagnose and troubleshoot unsuccessful health checks. The default value is `no`.

  The options are:

  • **no**
    
    Specifies that the system does not redirect error messages and additional information related to this monitor.

  • **yes**
    
    Specifies that the system redirects error messages and additional information to the `/var/log/<monitor_type>_<ip address>_<port>.log` file.

◆ **defaults-from**

  Specifies the name of the monitor from which you want your custom monitor to inherit settings. The default value is `radius`.

◆ **description**

  User-defined description.
destination
Specifies the IP address and service port of the resource that is the
destination of this monitor. The default value is *:*.
Possible values are:
- *:*  
  Specifies that the system marks a pool member up or down based on
  the response of the server at the IP address and port supplied by the
  pool member.
- *:port  
  Specifies that the system marks a pool member up or down based on
  the response of the server at the IP address supplied by the pool
  member and the port you specify.
- <IP address>:<port>  
  Specifies that the system marks a pool member up or down based on
  the response of the server at the IP address and port you specify.

glob
Displays the items that match the glob expression. For a description of
glob expression syntax, see the glob man page.

interval
Specifies, in seconds, the frequency at which the system issues the
monitor check when either the resource is down or the status of the
resource is unknown. The default value is 10 seconds.

manual-resume
Specifies whether the system automatically changes the status of a
resource to up at the next successful monitor check. The default value of
the manual-resume option is disabled.
If you set the manual-resume option to enabled, you must manually
mark the resource as up before the system can use it for load balancing
connections.

name
Specifies a unique name for the component. This option is required for
the commands create, delete, and modify.

nas-ip-address
Specifies the network access server IP address that the system uses to
identify itself to the RADIUS server. With this option, multiple BIG-IP
systems can appear as a single network access device to the RADIUS
server. The default value is none.

partition
Displays the administrative partition in which the component resides.

regex
Displays the items that match the regular expression. The regular
expression must be preceded by an at sign (@[regular expression]) to
indicate that the identifier is a regular expression. For a description of
regular expression syntax, see the regex man page.

secret
Specifies the secret the monitor must use when contacting the resource.
The default value is none.
◆ **time-until-up**
   Specifies the amount of time in seconds after the first successful response before a node is marked up. A value of 0 (zero) causes a node to be marked up immediately after a valid response is received from the node. The default value is 0 (zero).

◆ **timeout**
   Specifies the number of seconds the target has in which to respond to the monitor request. The default value is 31 seconds.
   If the target responds within the set time period, it is considered *up*. If the target does not respond within the set time period, it is considered *down*. Also, if the target responds with a RESET packet, the system immediately flags the target as *down* without waiting for the timeout interval to expire.

◆ **up-interval**
   Specifies, in seconds, the frequency at which the system issues the monitor check when the resource is *up*. The default value is 0 (zero), which specifies that the system uses the value of the *interval* option whether the resource is *up* or *down*.

   **Important:** F5 Networks recommends that when you configure this option and the *interval* option, that the value that is greater be a multiple of the lesser value to allow for an even distribution of monitor checks among all monitors.

◆ **username**
   Specifies the user name if the monitored target requires authentication. The default value is none.

---

**See also**

create, delete, edit, glob, list, modify, regex, show, tmsh
real-server

Configures a RealServer® monitor.

Module

ltm monitor

Syntax

Configure the real-server component within the ltm monitor module using the following syntax.

Create/Modify

create real-server [name]
modify real-server [name]
   options:
      defaults-from [name]
      description [string]
      interval [integer]
      metrics [ metrics ] | none
      time-until-up [integer]
      timeout [integer]

edit real-server [ [ [name] | [glob] | [regex] ] ... ]
   options:
      all-properties
      non-default-properties

Display

list real-server
list real-server [name]
show running-config real-server
show running-config real-server [name]
   options:
      agent
      all-properties
      command
      method
      non-default-properties
      one-line
      partition
Delete

`delete real-server [name]`

**Note**

You cannot delete default monitors.

Description

You can use the `real-server` component to configure a custom monitor, or you can use the default RealServer monitor that Local Traffic Manager provides. This type of monitor checks the performance of a pool, pool member, or virtual server that is running the RealServer data collection agent, and then dynamically load balances traffic accordingly.

Examples

Creates a monitor named `my_real-server` that inherits properties from the default RealServer monitor.

```
create real-server my_real-server defaults-from real_server
```

Displays the properties of all of the RealServer monitors:

```
list real-server
```

Options

You can use these options with the `real-server` component:

- **agent**
  Displays the agent for the monitor. The default agent is Mozilla/4.0 (compatible: MSIE 5.0; Windows NT). You cannot modify the agent.

- **command**
  Displays the command that the system uses to obtain the metrics from the resource. See the documentation for this resource for information on available commands.

- **defaults-from**
  Specifies the name of the monitor from which you want your custom monitor to inherit settings. The default value is `real_server`.

- **description**
  User-defined description.

- **interval**
  Specifies the frequency at which the system issues the monitor check. The default value is 5 seconds.

- **name**
  Specifies a unique name for the component. This option is required.
Chapter 31

- **method**
  Displays the GET method. You cannot modify the method.

- **metrics**
  Specifies the performance metrics that the commands collect from the target. The default value is `ServerBandwidth:1.5, CPUPercentUsage, MemoryUsage, TotalClientCount`.

- **partition**
  Displays the administrative partition in which the component resides.

- **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. For a description of regular expression syntax, see the `regex` man page.

- **time-until-up**
  Specifies the amount of time, in seconds, after the first successful response before a node is marked up. A value of 0 (zero) causes a node to be marked up immediately after a valid response is received from the node. The default value is 0 (zero).

- **timeout**
  Specifies the number of seconds the target has in which to respond to the monitor request. The default value is 16 seconds.

  If the target responds within the set time period, it is considered up. If the target does not respond within the set time period, it is considered down. Also, if the target responds with a RESET packet, the system immediately flags the target as down without waiting for the timeout interval to expire.

See also

create, delete, edit, glob, list, modify, regex, show, tmsh
rpc

Configures a Remote Procedure Call (RPC) monitor.

Module

ltm monitor

Syntax

Configure the rpc component within the ltm monitor module using the following syntax.

Create/Modify

create rpc [name]
modify rpc [name]

options:
  debug [no | yes]
  defaults-from [name]
  description [string]
  destination [ip address] [port]
  interval [integer]
  manual-resume [enabled | disabled]
  mode [tcp | udp]
  program-number [ [integer] | none]
  time-until-up [integer]
  timeout [integer]
  up-interval [integer]
  version-number [ [integer] | none]

edit rpc [ [ [name] | [glob] | [regex] ] ... ]

options:
  all-properties
  non-default-properties

Display

list rpc
list rpc [ [ [name] | [glob] | [regex] ] ... ]

show running-config rpc
show running-config rpc [ [ [name] | [glob] | [regex] ] ... ]

options:
  all-properties
  non-default-properties
  one-line
  partition
Delete

delete rpc [name]

◆ Note

You cannot delete default monitors.

Description

You can use the rpc component to configure a custom monitor, or you can use the default Scripted monitor that Local Traffic Manager provides. This type of monitor queries the RPC server and verifies the availability of a given program.

Examples

Creates a monitor named my_rpc that inherits properties from the default RPC monitor.

create rpc my_rpc defaults-from rpc

Displays the properties of all of the RPC monitors:

list rpc

Options

You can use these options with the rpc component:

◆ debug

Specifies whether the monitor sends error messages and additional information to a log file created and labeled specifically for this monitor. You can use the log information to help diagnose and troubleshoot unsuccessful health checks. The default value is no.

The options are:

• no

  Specifies that the system does not redirect error messages and additional information related to this monitor.

• yes

  Specifies that the system redirects error messages and additional information to the

  /var/log/<monitor_type>_<ip address>.<port>.log file.

◆ defaults-from

  Specifies the name of the monitor from which you want your custom monitor to inherit settings. The default value is rpc.

◆ description

  User-defined description.
◆ **destination**
  Specifies the IP address and service port of the resource that is the destination of this monitor. The default value is `*:*`.
  Possible values are:
  - `*: *
    Specifies that the system marks a pool member **up** or **down** based on the response of the server at the IP address and port supplied by the pool member.
  - `*:port
    Specifies that the system marks a pool member **up** or **down** based on the response of the server at the IP address supplied by the pool member and the port you specify.
  - `<IP address>:<port>
    Specifies that the system marks a pool member **up** or **down** based on the response of the server at the IP address and port you specify.

◆ **glob**
  Displays the items that match the glob expression. For a description of glob expression syntax, see the glob man page.

◆ **interval**
  Specifies, in seconds, the frequency at which the system issues the monitor check when either the resource is **down** or the status of the resource is unknown. The default value is 10 seconds.

◆ **manual-resume**
  Specifies whether the system automatically changes the status of a resource to **up** at the next successful monitor check. The default value of the manual-resume option is disabled.
  If you set the manual-resume option to enabled, you must manually mark the resource as **up** before the system can use it for load balancing connections.

◆ **mode**
  Specifies the protocol that the monitor uses to communicate with the target. The default value is tcp.
  The options are:
  - **tcp**
    Specifies that the monitor uses the TCP protocol to communicate with the target object.
  - **udp**
    Specifies that the monitor uses the UDP protocol to communicate with the target object.

◆ **name**
  Specifies a unique name for the component. This option is required for the commands create, delete, and modify.

◆ **partition**
  Displays the administrative partition in which the component resides.
◆ **program-number**
   Specifies the number of the program for which you want the monitor to verify availability. The default value is **none**.

◆ **regex**
   Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. For a description of regular expression syntax, see the **regex** man page.

◆ **time-until-up**
   Specifies the amount of time, in seconds, after the first successful response before a node is marked **up**. A value of 0 (zero) causes a node to be marked **up** immediately after a valid response is received from the node. The default value is 0 (zero).

◆ **timeout**
   Specifies the number of seconds the target has in which to respond to the monitor request. The default value is 31 seconds.
   
   If the target responds within the set time period, it is considered **up**. If the target does not respond within the set time period, it is considered **down**. Also, if the target responds with a RESET packet, the system immediately flags the target as **down** without waiting for the timeout interval to expire.

◆ **up-interval**
   Specifies, in seconds, the frequency at which the system issues the monitor check when the resource is **up**. The default value is 0 (zero), which specifies that the system uses the value of the **interval** option whether the resource is **up** or **down**.

   **Important:** F5 Networks recommends that when you configure this option and the **interval** option, that the value that is greater be a multiple of the lesser value to allow for an even distribution of monitor checks among all monitors.

◆ **version-number**
   Specifies the number of the version of the program for which you want the monitor to verify availability. The default value is **none**.

---

**See also**

create, delete, edit, glob, list, modify, regex, show, tmsh
sasp

Configures a Simple Access Signaling Protocol (SASP) monitor.

Module

ltm monitor

Syntax

Configure the sasp component within the ltm monitor module using the following syntax.

Create/Modify

create sasp [name]
modify sasp [name]
options:
  address [ [ip address] | none]
  defaults-from [name]
  description [string]
  interval [integer]
  protocol [tcp | udp]
  service [none | [port] ]
  time-until-up [integer]
  timeout [integer]
edit sasp [ [ [name] | [glob] | [regex] ] ... ]
options:
  all-properties
  non-default-properties

Display

list sasp
list sasp [ [ [name] | [glob] | [regex] ] ... ]
show running-config sasp
show running-config sasp [ [ [name] | [glob] | [regex] ] ... ]
options:
  all-properties
  non-default-properties
  one-line
  partition
Delete

```bash
delete sasp [name]
```

◆ Note

*You cannot delete default monitors.*

Description

You can use the `sasp` component to configure a custom monitor, or you can use the default Scripted monitor that Local Traffic Manager provides. This type of monitor verifies the availability of IBM Group Workload Managers network resources.

Examples

Creates a monitor named `my_sasp` that inherits properties from the default SASP monitor.

```bash
create sasp my_sasp defaults-from sasp
```

Displays the properties of all of the SASP monitors:

```bash
list sasp
```

Options

You can use these options with the `sasp` component:

- **address**
  Specifies the IP address of the Group Workload Manager.

- **defaults-from**
  Specifies the name of the monitor from which you want your custom monitor to inherit settings. The default value is `sasp`.

- **description**
  User-defined description.

- **glob**
  Displays the items that match the `glob` expression. For a description of `glob` expression syntax, see the `glob` man page.

- **interval**
  Specifies the frequency at which the system issues the monitor check. The default value is `auto`.

- **name**
  Specifies a unique name for the component. This option is required for the commands `create`, `delete`, and `modify`.

- **partition**
  Displays the administrative partition in which the component resides.
◆ **protocol**
   Specifies the protocol that the monitor uses to communicate with the target. The default value is `tcp`.

◆ **regex**
   Displays the items that match the regular expression. The regular expression must be preceded by an at sign (`@`[regular expression]) to indicate that the identifier is a regular expression. For a description of regular expression syntax, see the `regex` man page.

◆ **service**
   Specifies the port through which the SASP monitor communicates with the Group Workload Manager. The default port is `3000`.

◆ **time-until-up**
   Specifies the amount of time, in seconds, after the first successful response before a node is marked **up**. A value of `0` (zero) causes a node to be marked **up** immediately after a valid response is received from the node. The default value is `0` (zero).

◆ **timeout**
   Specifies the number of seconds the target has in which to respond to the monitor request. The default value is `100` seconds.

   If the target responds within the set time period, it is considered **up**. If the target does not respond within the set time period, it is considered **down**. Also, if the target responds with a RESET packet, the system immediately flags the target as **down** without waiting for the timeout interval to expire.

### See also

`create`, `delete`, `edit`, `glob`, `list`, `modify`, `regex`, `show`, `tmsh`
scripted

Configures a Scripted monitor.

Module

ltm monitor

Syntax

Configure the scripted component within the ltm monitor module using the following syntax.

Create/Modify

```
create scripted [name]
modify scripted [name]
```

**options:**
- `debug [no | yes]`
- `defaults-from [name]`
- `description [string]`
- `destination [ip address] [port]`
- `filename [ [filename] | none]`
- `interval [integer]`
- `manual-resume [enabled | disabled]`
- `time-until-up [integer]`
- `timeout [integer]`
- `up-interval [integer]`

```
edit scripted [ [ [name] | [glob] | [regex] ] ... ]
edit scripted [ [ [name] | [glob] | [regex] ] ... ]
```

**options:**
- `all-properties`
- `non-default-properties`

Display

```
list scripted
list scripted [ [ [name] | [glob] | [regex] ] ... ]
show running-config scripted
show running-config scripted [ [ [name] | [glob] | [regex] ] ... ]
```

**options:**
- `all-properties`
- `non-default-properties`
- `one-line`
- `partition`
Delete

```
delete scripted [name]
```

◆ Note

*You cannot delete default monitors.*

Description

You can use the `scripted` component to configure a custom monitor, or you can use the default Scripted monitor that Local Traffic Manager provides.

Examples

Creates a monitor named `my_scripted` that inherits properties from the default Scripted monitor.
```
create scripted my_scripted defaults-from scripted
```

Displays the properties of all of the Scripted monitors:
```
list scripted
```

Options

You can use these options with the `scripted` component:

◆ debug
  Specifies whether the monitor sends error messages and additional information to a log file created and labeled specifically for this monitor. You can use the log information to help diagnose and troubleshoot unsuccessful health checks. The default value is **no**.
  
The options are:
  
  • **no**
    Specifies that the system does not redirect error messages and additional information related to this monitor.
  
  • **yes**
    Specifies that the system redirects error messages and additional information to the
    
    `/var/log/<monitor_type>_<ip address>.<port>.log`

◆ defaults-from
  Specifies the name of the monitor from which you want your custom monitor to inherit settings. The default value is **scripted**.

◆ description
  User-defined description.
◆ destination
Specifies the IP address and service port of the resource that is the destination of this monitor. The default value is *:*.
Possible values are:
- *:*  
  Specifies that the system marks a pool member up or down based on the response of the server at the IP address and port supplied by the pool member.
- *:port  
  Specifies that the system marks a pool member up or down based on the response of the server at the IP address supplied by the pool member and the port you specify.
- <IP address>:<port>  
  Specifies that the system marks a pool member up or down based on the response of the server at the IP address and port you specify.
◆ filename  
Specifies the name of a file in the /config/eav/ directory on the system. The user-created file contains the send and expect data that the monitor uses for the monitor check. The default value is none.
◆ glob  
Displays the items that match the glob expression. For a description of glob expression syntax, see the glob man page.
◆ interval  
Specifies, in seconds, the frequency at which the system issues the monitor check when either the resource is down or the status of the resource is unknown. The default value is 10 seconds.
◆ manual-resume  
Specifies whether the system automatically changes the status of a resource to up at the next successful monitor check. The default value of the manual-resume option is disabled.
If you set the manual-resume option to enabled, you must manually mark the resource as up before the system can use it for load balancing connections.
◆ name  
Specifies a unique name for the component. This option is required for the commands create, delete, and modify.
◆ partition  
Displays the administrative partition in which the component resides.
◆ regex  
Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. For a description of regular expression syntax, see the regex man page.
◆ **time-until-up**
   Specifies the amount of time, in seconds, after the first successful response before a node is marked **up**. A value of 0 (zero) causes a node to be marked **up** immediately after a valid response is received from the node. The default value is 0 (zero).

◆ **timeout**
   Specifies the number of seconds the target has in which to respond to the monitor request. The default value is 31 seconds.
   If the target responds within the set time period, it is considered **up**. If the target does not respond within the set time period, it is considered **down**. Also, if the target responds with a RESET packet, the system immediately flags the target as **down** without waiting for the timeout interval to expire.

◆ **up-interval**
   Specifies, in seconds, the frequency at which the system issues the monitor check when the resource is **up**. The default value is 0 (zero), which specifies that the system uses the value of the **interval** option whether the resource is **up** or **down**.

   **Important:** F5 Networks recommends that when you configure this option and the **interval** option, that the value that is greater be a multiple of the lesser value to allow for an even distribution of monitor checks among all monitors.

**See also**

create, delete, edit, glob, list, modify, regex, show, tmsh
Chapter 31

sip

Configures a Session Initiation Protocol (SIP) monitor.

Module

ltm monitor

Syntax

Configure the sip component within the ltm monitor module using the following syntax.

Create/Modify

create sip [name]
modify sip [name]

options:
cert [ [cert list] | none]
cipherlist [string]
compatibility [enabled | disabled ]
debug [no | yes]
defaults-from [name]
description [string]
destination [ip address][port]
filter [any | none | status]
filter-neg [any | none | status]
headers [ [new line separated headers] | none]
interval [integer]
key [ [key] | none]
manual-resume [enabled | disabled]
mode [sips | tcp | tls | udp]
request [none | [string] ]
time-until-up [integer]
up-interval [integer]
username [ [name] | none]

edit sip [ [ [name] | [glob] | [regex] ] ... ]

options:
all-properties
non-default-properties
Display

list sip
list sip [ [ [name] | [glob] | [regex] ] ... ]
show running-config sip
show running-config sip [ [ [name] | [glob] | [regex] ] ... ]
options:
  all-properties
  non-default-properties
  one-line
  partition

Delete

delete sip [name]

◆ Note
You cannot delete default monitors.

Description

You can use the sip component to configure a custom monitor, or you can use the default SIP monitor that Local Traffic Manager provides. This type of monitor checks the status of SIP Call-ID services on a device. The SIP protocol enables real-time messaging, voice, data, and video.

Examples

Creates a monitor named my_sip that inherits properties from the default SIP monitor.
create sip my_sip defaults-from sip

Displays the properties of all of the SIP monitors:
list sip

Options

You can use these options with the sip component:

◆ cert
  Specifies a fully-qualified path for a client certificate that the monitor sends to the target SSL server. The default value is none.

◆ cipherlist
  Specifies the list of ciphers for this monitor. The default value is DEFAULT:+SHA:+3DES:+kEDH.
 compatibility
Specifications, when enabled, that the SSL options setting (in OpenSSL) is set to ALL. The default value is enabled.

deadbeef
Specifies whether the monitor sends error messages and additional information to a log file created and labeled specifically for this monitor. You can use the log information to help diagnose and troubleshoot unsuccessful health checks. The default value is no.
The options are:

- **no**
  Specifies that the system does not redirect error messages and additional information related to this monitor.

- **yes**
  Specifies that the system redirects error messages and additional information to the /var/log/<monitor name>

defaults-from
Specifies the name of the monitor from which you want your custom monitor to inherit settings. The default value is sip.

description
User-defined description.

destination
Specifies the IP address and service port of the resource that is the destination of this monitor. The default value is *:*.
Possible values are:

- ***:**
  Specifies that the system marks a pool member **up** or **down** based on the response of the server at the IP address and port supplied by the pool member.

- **:*:port**
  Specifies that the system marks a pool member **up** or **down** based on the response of the server at the IP address supplied by the pool member and the port you specify.

- **<IP address>:<port>**
  Specifies that the system marks a pool member **up** or **down** based on the response of the server at the IP address and port you specify.

filter
Specifies the SIP status codes that the target can return to be considered **up**. By default, the system always accepts status codes whose value is in the 100, 200, or 300s.
The options are:

- **any**
  Specifies that the monitor accepts any SIP status codes.

- **none**
  Specifies that the monitor does not accept any other SIP status codes. This is the default value.
• **status**
  Specifies one or more status codes that you want to add to the monitor.

• **filter-neg**
  Specifies the SIP status codes that the target can return to be considered down. By default, the system always accepts status codes according to `sip-monitor.filter`. After checking that, the status code is checked against this key. If a code is also in `sip-monitor.filter`, the node is marked up.

The options are:

• **any**
  Specifies that the monitor rejects all SIP status codes that are not in `sip-monitor.filter`.

• **none**
  Specifies that the monitor does not specifically reject any other SIP status codes. This is the default value.

• **status**
  Specifies one or more status codes that you want to add to the monitor.

• **glob**
  Displays the items that match the glob expression. For a description of glob expression syntax, see the glob man page.

• **headers**
  Specifies the set of SIP headers in the SIP message that is sent to the target. Separate each header with a new line. The default value is none.

• **interval**
  Specifies, in seconds, the frequency at which the system issues the monitor check when either the resource is down or the status of the resource is unknown. The default value is 5 seconds.

• **key**
  Specifies the key if the monitored target requires authentication. The default value is none.

• **manual-resume**
  Specifies whether the system automatically changes the status of a resource to up at the next successful monitor check. The default value of the manual-resume option is disabled.

  If you set the manual-resume option to enabled, you must manually mark the resource as up before the system can use it for load balancing connections.

• **mode**
  Specifies the protocol that the monitor uses to communicate with the target.

  The options are:

• **sip**
  Specifies that the monitor uses SIPS to communicate with the target.
- **tcp**
  Specifies that the monitor uses TCP to communicate with the target.

- **tls**
  Specifies that the monitor uses TLS to communicate with the target, and the SIP URI is SIPS.

- **udp**
  Specifies that the monitor uses UDP to communicate with the target. This is the default value.

- **name**
  Specifies a unique name for the component. This option is required for the commands `create`, `delete`, and `modify`.

- **partition**
  Displays the administrative partition in which the component resides.

- **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. For a description of regular expression syntax, see the `regex` man page.

- **request**
  Specifies the SIP request line in the SIP message that is sent to the target. The default value is `none`.

- **time-until-up**
  Specifies the amount of time, in seconds, after the first successful response before a node is marked **up**. A value of 0 (zero) causes a node to be marked **up** immediately after a valid response is received from the node. The default value is 0 (zero).

- **timeout**
  Specifies the number of seconds the target has in which to respond to the monitor request. The default value is 16 seconds.

  If the target responds within the set time period, it is considered **up**. If the target does not respond within the set time period, it is considered **down**. Also, if the target responds with a RESET packet, the system immediately flags the target as **down** without waiting for the timeout interval to expire.

- **up-interval**
  Specifies, in seconds, the frequency at which the system issues the monitor check when the resource is **up**. The default value is 0 (zero), which specifies that the system uses the value of the **interval** option whether the resource is **up** or **down**.

  **Important:** F5 Networks recommends that when you configure this option and the **interval** option, that the value that is greater be a multiple of the lesser value to allow for an even distribution of monitor checks among all monitors.
See also

create, delete, edit, glob, list, modify, regex, show, tmsh
smb

Configures a Server Message Bloc (SMB)/Common Internet File System (CIFS) monitor.

Module

ltm monitor

Syntax

Configure the smb component within the ltm monitor module using the following syntax.

Create/Modify

```plaintext
create smb [name]
modify smb [name]
  options:
    debug [no | yes]
    defaults-from [name]
    description [string]
    destination [ip address][port]
    get [none | [filename] ]
    interval [integer]
    manual-resume [enabled | disabled]
    password [none | [password] ]
    server [ [NETBIOS name] | none]
    service [ [ [name] | [integer] ] | none]
    time-until-up [integer]
    timeout [integer]
    up-interval [integer]
    username [ [name] | none]
edit smb [ [ [name] | [glob] | [regex] ] ... ]
  options:
    all-properties
    non-default-properties
```

Display

```plaintext
list smb
list smb [ [ [name] | [glob] | [regex] ] ... ]
show running-config smb
show running-config smb [ [ [name] | [glob] | [regex] ] ... ]
  options:
```
all-properties
non-default-properties
one-line
partition

Delete

delete smb [name]

◆ Note
You cannot delete default monitors.

Description

You can use the smb component to configure a custom monitor, or you can use the default SMB monitor that Local Traffic Manager provides. This type of monitor verifies the availability of an SMB/CIFS server. You can use this type of monitor to check the availability of the server as a whole, the availability of a specific service on the server, or the availability of a specific file used by a service.

Examples

Creates a monitor named my_smb that inherits properties from the default SMB monitor.
create smb my_smb defaults-from smb

Displays the properties of all of the SMB monitors:
list smb

Options

You can use these options with the smb component:

◆ debug
  Specifies whether the monitor sends error messages and additional information to a log file created and labeled specifically for this monitor. You can use the log information to help diagnose and troubleshoot unsuccessful health checks. The default value is no.
  The options are:
  • no
    Specifies that the system does not redirect error messages and additional information related to this monitor.
• yes
  Specifies that the system redirects error messages and additional information to the
  /var/log/<monitor_type>_<ip address>_<port>_.log file.

◆ defaults-from
  Specifies the name of the monitor from which you want your custom monitor to inherit settings. The default value is smb.

◆ description
  User-defined description.

◆ destination
  Specifies the IP address and service port of the resource that is the destination of this monitor. The default value is *:*.
  Possible values are:
  • *:*
    Specifies that the system marks a pool member up or down based on the response of the server at the IP address and port supplied by the pool member.
  • *:<port>
    Specifies that the system marks a pool member up or down based on the response of the server at the IP address supplied by the pool member and the port you specify.
  • <IP address>:<port>
    Specifies that the system marks a pool member up or down based on the response of the server at the IP address and port you specify.

◆ get
  Specifies a file associated with a service. The default value is none.
  The monitor uses the relative path to the service itself when attempting to locate the file. You are not required to specify a value for this option; however, if you elect to use this option you must also specify a value for the service option.

◆ glob
  Displays the items that match the glob expression. For a description of glob expression syntax, see the glob man page.

◆ interval
  Specifies, in seconds, the frequency at which the system issues the monitor check when either the resource is down or the status of the resource is unknown. The default value is 10 seconds.

◆ manual-resume
  Specifies whether the system automatically changes the status of a resource to up at the next successful monitor check. The default value of the manual-resume option is disabled.
  If you set the manual-resume option to enabled, you must manually mark the resource as up before the system can use it for load balancing connections.

◆ name
  Specifies a unique name for the component. This option is required for the commands create, delete, and modify.
partition  
Displays the administrative partition in which the component resides.

password  
Specifies the password if the monitored target requires authentication. The default value is none.

regex  
Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. For a description of regular expression syntax, see the regex man page.

server  
Specifies the NetBIOS name of the SMB/CIFS server for which this monitor checks for availability. You must specify a server for this monitor to function. The default value is none.

service  
Specifies a specific service on the SMB/CIFS for which you want to verify availability. The default value is none.

time-until-up  
Specifies the amount of time, in seconds, after the first successful response before a node is marked up. A value of 0 (zero) causes a node to be marked up immediately after a valid response is received from the node. The default value is 0 (zero).

timeout  
Specifies the number of seconds the target has in which to respond to the monitor request. The default value is 31 seconds.

Important: F5 Networks recommends that when you configure this option and the interval option, that the value that is greater be a multiple of the lesser value to allow for an even distribution of monitor checks among all monitors.

username  
Specifies the user name if the monitored target requires authentication. The default value is none.

See also
create, delete, edit, glob, list, modify, regex, show, tmsh
smtp

Configures a Simple Mail Transport Protocol (SMTP) monitor.

Module

ltm monitor

Syntax

Configure the smtp component within the ltm monitor module using the following syntax.

Create/Modify

create smtp [name]
modify smtp [name]

options:
  debug [no | yes]
  defaults-from [name]
  description [string]
  destination [ip address][port]
  domain [ [name] | none]
  interval [integer]
  manual-resume [enabled | disabled]
  time-until-up [integer]
  timeout [integer]
  up-interval [integer]

edit smtp [ [ [name] | [glob] | [regex] ] ... ]

options:
  all-properties
  non-default-properties

Display

list smtp
list smtp [ [ [name] | [glob] | [regex] ] ... ]
show running-config smtp
show running-config smtp [ [ [name] | [glob] | [regex] ] ... ]

options:
  all-properties
  non-default-properties
  one-line
  partition
Delete

```
delete smtp [name]
```

◆ Note

_You cannot delete default monitors._

Description

You can use the `smtp` component to configure a custom monitor, or you can use the default SMTP monitor that Local Traffic Manager provides. This type of monitor checks the status of a pool, pool member, or virtual server by issuing standard SMTP commands.

Examples

Creates a monitor named `my_smtp` that inherits properties from the default SMTP monitor.

```
create smtp my_smtp defaults-from smtp
```

Displays the properties of all of the SMTP monitors:

```
list smtp
```

Options

You can use these options with the `smtp` component:

◆ `debug`
   Specifies whether the monitor sends error messages and additional information to a log file created and labeled specifically for this monitor. You can use the log information to help diagnose and troubleshoot unsuccessful health checks. The default value is `no`.
   
   The options are:
   
   •  `no`
      Specifies that the system does not redirect error messages and additional information related to this monitor.
   
   •  `yes`
      Specifies that the system redirects error messages and additional information to the
      `/var/log/<monitor_type>_<ip address><port>.log` file.

◆ `defaults-from`
   Specifies the name of the monitor from which you want your custom monitor to inherit settings. The default value is `smtp`.

◆ `description`
   User-defined description.
- **destination**
  Specifies the IP address and service port of the resource that is the destination of this monitor. The default value is `*:*

Possible values are:
- `*:*
  Specifies that the system marks a pool member **up** or **down** based on the response of the server at the IP address and port supplied by the pool member.
- `*:port`
  Specifies that the system marks a pool member **up** or **down** based on the response of the server at the IP address supplied by the pool member and the port you specify.
- `<IP address>:<port>`
  Specifies that the system marks a pool member **up** or **down** based on the response of the server at the IP address and port you specify.

- **domain**
  Specifies the domain name to check, for example: **bigipinternal.com**. The default value is none.

- **glob**
  Displays the items that match the glob expression. For a description of glob expression syntax, see the glob man page.

- **interval**
  Specifies, in seconds, the frequency at which the system issues the monitor check when either the resource is **down** or the status of the resource is unknown. The default value is 5 seconds.

- **manual-resume**
  Specifies whether the system automatically changes the status of a resource to **up** at the next successful monitor check. The default value of the manual-resume option is disabled.

  If you set the manual-resume option to enabled, you must manually mark the resource as **up** before the system can use it for load balancing connections.

- **name**
  Specifies a unique name for the component. This option is required for the commands **create**, **delete**, and **modify**.

- **partition**
  Displays the administrative partition in which the component resides.

- **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. For a description of regular expression syntax, see the regex man page.

- **time-until-up**
  Specifies the amount of time, in seconds, after the first successful response before a node is marked **up**. A value of 0 (zero) causes a node to be marked **up** immediately after a valid response is received from the node. The default value is 0 (zero).
timeout
Specifies the number of seconds the target has in which to respond to the monitor request. The default value is 16 seconds.
If the target responds within the set time period, it is considered *up*. If the target does not respond within the set time period, it is considered *down*. Also, if the target responds with a RESET packet, the system immediately flags the target as *down* without waiting for the timeout interval to expire.

up-interval
Specifies, in seconds, the frequency at which the system issues the monitor check when the resource is *up*. The default value is 0 (zero), which specifies that the system uses the value of the interval option whether the resource is *up* or *down*.

Important: F5 Networks recommends that when you configure this option and the interval option, that the value that is greater be a multiple of the lesser value to allow for an even distribution of monitor checks among all monitors.

See also

create, delete, edit, glob, list, modify, regex, show, tmsh
snmp-dca

Configures a Simple Network Management Protocol (SNMP) Data Center Audit monitor.

Module

ltm monitor

Syntax

Configure the snmp-dca component within the ltm monitor module using the following syntax.

Create/Modify

create snmp-dca [name]
modify snmp-dca [name]

options:
  agent-type [generic | other | win2000 | ucd]
  community [ [name] | none]
  cpu-coefficient [ [integer] | none]
  cpu-threshold [none | [integer] ]
  defaults-from [name]
  description [string]
  disk-coefficient [ [integer] | none]
  disk-threshold [none | [integer] ]
  interval [integer]
  memory-coefficient [ [integer] | none]
  memory-threshold [none | [integer] ]
  port [ [integer] | none]
  time-until-up [integer]
  timeout [integer]
  user-defined
  version [ [integer] | none]
edit snmp-dca [ [name] | [glob] | [regex] ] ...

options:
  all-properties
  non-default-properties
Display

list snmp-dca
list snmp-dca [ [ name ] | [ glob ] | [ regex ] ... ]
show running-config snmp-dca
show running-config snmp-dca [ [ name ] | [ glob ] | [ regex ] ... ]
options:
   all-properties
   non-default-properties
   one-line
   partition

Delete

delete snmp-dca [ name ]

◆ Note

You cannot delete default monitors.

Description

You can use the snmp-dca component to configure a custom monitor, or you can use the default SNMP DCA monitor that Local Traffic Manager provides. This type of monitor checks the performance of a server running an SNMP agent such as UC Davis, for the purpose of load balancing traffic to that server.

Examples

Creates a monitor named my_snmp-dca that inherits properties from the default SNMP DCA monitor.
create snmp-dca my_snmp-dca defaults-from snmp_dca

Displays the properties of all of the SNMP DCA monitors:
list snmp

Options

You can use these options with the snmp-dca component:
◆ agent-type
   Specifies the type of agent. The default value is ucd.
◆ community
   Specifies the community name that the BIG-IP system must use to authenticate with the host server through SNMP. The default value is public.
◆ **cpu-coefficient**
Specifies the coefficient that the system uses to calculate the weight of the CPU threshold in the dynamic ratio load balancing algorithm. The default value is **1.5**.

◆ **cpu-threshold**
Specifies the maximum acceptable CPU usage on the target server. The default value is **80** percent.

◆ **defaults-from**
Specifies the name of the monitor from which you want your custom monitor to inherit settings. The default value is **snmp_dca**.

◆ **description**
User-defined description.

◆ **disk-coefficient**
Specifies the coefficient that the system uses to calculate the weight of the disk threshold in the dynamic ratio load balancing algorithm. The default value is **2.0**.

◆ **disk-threshold**
Specifies the maximum acceptable disk usage on the target server. The default value is **90** percent.

◆ **glob**
Displays the items that match the **glob** expression. For a description of **glob** expression syntax, see the **glob man page**.

◆ **interval**
Specifies the frequency at which the system issues the monitor check. The default value is **10** seconds.

◆ **memory-coefficient**
Specifies the coefficient that the system uses to calculate the weight of the memory threshold in the dynamic ratio load balancing algorithm. The default value is **1.0**.

◆ **memory-threshold**
Specifies the maximum acceptable memory usage on the target server. The default value is **70** percent.

◆ **name**
Specifies a unique name for the component. This option is required for the commands **create**, **delete**, and **modify**.

◆ **partition**
Displays the administrative partition in which the component resides.

◆ **port**
Specifies the port number to which this monitor sends SNMP traps. The default value is **none**.

◆ **regex**
Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. For a description of regular expression syntax, see the **regex man page**.
◆ **time-until-up**
   Specifies the amount of time, in seconds, after the first successful response before a node is marked *up*. A value of 0 (zero) causes a node to be marked *up* immediately after a valid response is received from the node. The default value is 0 (zero).

◆ **timeout**
   Specifies the number of seconds the target has in which to respond to the monitor request. The default value is 30 seconds.
   If the target responds within the set time period, it is considered *up*. If the target does not respond within the set time period, it is considered *down*. Also, if the target responds with a RESET packet, the system immediately flags the target as *down* without waiting for the timeout interval to expire.

◆ **user-defined**
   Specifies any user-defined command-line arguments and variables that the external program requires. The default value is *none*.

◆ **version**
   Specifies the version of SNMP that the host server uses. The default value is *none*.

### See also

create, delete, edit, glob, list, modify, regex, show, tmsh
**snmp-dca-base**

Configures a base Simple Network Management Protocol (SNMP) Data Center Audit monitor.

**Module**

`ltm monitor`

**Syntax**

Configure the `snmp-dca-base` component within the `ltm monitor` module using the following syntax.

**Create/Modify**

```plaintext
create snmp-dca-base [name]
modyf snmp-dca-base [name]

options:
  community [ [name] | none]
  cpu-coefficient [ [integer] | none]
  defaults-from [name]
  description [string]
  interval [integer]
  time-until-up [integer]
  timeout [integer]
  user-defined [ [name] [value] | [name] none ]
  version [ [integer] | none]

edit snmp-dca-base [ [ [name] | [glob] | [regex] ] ... ]

options:
  all-properties
  non-default-properties
```

**Display**

```plaintext
list snmp-dca-base
list snmp-dca-base [ [name] | [glob] | [regex] ] ... 
show running-config snmp-dca-base
show running-config snmp-dca-base [ [name] | [glob] | [regex] ] ... 

options:
  all-properties
  non-default-properties
  one-line
  partition
```
Delete

```
delete snmp-dca-base [name]
```

◆ Note

*You cannot delete default monitors.*

Description

You can use the `snmp-dca-base` component to configure a custom monitor, or you can use the default base SNMP DCA monitor that Local Traffic Manager provides. This type of monitor checks the performance of servers that are running an SNMP agent, such as UC Davis. Use this monitor only when you want the load balancing destination to be based solely on user data, and not CPU, memory, or disk use.

Examples

- Creates a monitor named `my_snmp-dca-base` that inherits properties from the default base SNMP DCA monitor.

  ```
create snmp-dca-base my_snmp-dca-base defaults-from snmp_dca_base
  ```

- Displays the properties of all of the base SNMP DCA monitors:

  ```
  list snmp-dca-base
  ```

Options

You can use these options with the `snmp-dca` component:

- **community**
  Specifies the community name that the BIG-IP system must use to authenticate with the host server through SNMP. The default value is `public`.

- **defaults-from**
  Specifies the name of the monitor from which you want your custom monitor to inherit settings. The default value is `snmp_dca_base`.

- **description**
  User-defined description.

- **glob**
  Displays the items that match the `glob` expression. For a description of `glob` expression syntax, see the `glob` man page.

- **interval**
  Specifies the frequency at which the system issues the monitor check. The default value is 10 seconds.
◆ name
  Specifies a unique name for the component. This option is required for the commands create, delete, and modify.

◆ partition
  Displays the administrative partition in which the component resides.

◆ regex
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. For a description of regular expression syntax, see the regex man page.

◆ time-until-up
  Specifies the amount of time, in seconds, after the first successful response before a node is marked up. A value of 0 (zero) causes a node to be marked up immediately after a valid response is received from the node. The default value is 0 (zero).

◆ timeout
  Specifies the number of seconds the target has in which to respond to the monitor request. The default value is 30 seconds.
  If the target responds within the set time period, it is considered up. If the target does not respond within the set time period, it is considered down. Also, if the target responds with a RESET packet, the system immediately flags the target as down without waiting for the timeout interval to expire.

◆ user-defined
  Specifies attributes for a monitor that you define.
  Use the following syntax to specify a user defined parameter:
  ```sh
  modify external my_external user-defined my_param_name my_param_value
  ```
  Use the following syntax to remove a user defined parameter:
  ```sh
  modify external my_external user-defined my_param_name none
  ```

◆ version
  Specifies the version of SNMP that the host server uses. The default value is none.

See also

create, delete, edit, glob, list, ltm node, modify, regex, show, tmsh
soap

Configures a Simple Object Access Protocol (SOAP) monitor.

Module

ltm monitor

Syntax

Configure the soap component within the ltm monitor module using the following syntax.

Create/Modify

create soap [name]
modify soap [name]

options:
  debug [no | yes]
  defaults-from [name]
  description [string]
  destination [ip address][port]
  expect-fault [no | yes]
  interval [integer]
  manual-resume [enabled | disabled]
  namespace [ [name] | none]
  parameter-name [ [name] | none]
  parameter-type [bool | int | long | string ]
  parameter-value [none | [integer] | [string] ]
  password [none | [password] ]
  protocol [ http | [https] ]
  return-type [bool | char | double | int | long | none | short | [string] ]
  return-value [none | [integer] | [string] ]
  time-until-up [integer]
  timeout [integer]
  up-interval [integer]
  url-path [none | [string] ]
  username [ [name] | none]
edit soap [ [ [name] | [glob] | [regex] ] ... ]

options:
  all-properties
  non-default-properties
Display

```
list soap
list soap [ [ name ] | [ glob ] | [ regex ] ] ... ]
show running-config soap
show running-config soap [ [ name ] | [ glob ] | [ regex ] ] ... ]
```

options:
- all-properties
- method
- non-default-properties
- one-line
- partition

Delete

```
delete soap [ name ]
```

◆ Note

*You cannot delete default monitors.*

Description

You can use the `soap` component to configure a custom monitor, or you can use the default SOAP monitor that Local Traffic Manager provides. This type of monitor tests a web service based on SOAP.

Examples

Creates a monitor named `my_soap` that inherits properties from the default SOAP monitor.

```
create soap my_soap defaults-from soap
```

Displays the properties of all of the SOAP monitors:

```
list soap
```
## Options

You can use these options with the `soap` component:

- **debug**
  Specifies whether the monitor sends error messages and additional information to a log file created and labeled specifically for this monitor. You can use the log information to help diagnose and troubleshoot unsuccessful health checks. The default value is `no`.

  The options are:
  - **no**
    Specifies that the system does not redirect error messages and additional information related to this monitor.
  - **yes**
    Specifies that the system redirects error messages and additional information to the `/var/log/<monitor_type>_<ip address>.<port>.log` file.

- **defaults-from**
  Specifies the name of the monitor from which you want your custom monitor to inherit settings. The default value is `soap`.

- **description**
  User-defined description.

- **destination**
  Specifies the IP address and service port of the resource that is the destination of this monitor. The default value is `*:*`.

  Possible values are:
  - `*:*
    Specifies that the system marks a pool member **up** or **down** based on the response of the server at the IP address and port supplied by the pool member.
  - `*:port`
    Specifies that the system marks a pool member **up** or **down** based on the response of the server at the IP address supplied by the pool member and the port you specify.
  - `<IP address>:<port>`
    Specifies that the system marks a pool member **up** or **down** based on the response of the server at the IP address and port you specify.

- **expect-fault**
  Specifies whether the value of the `method` option causes the monitor to expect a SOAP fault message. The default value is `no`.

- **glob**
  Displays the items that match the `glob` expression. For a description of `glob` expression syntax, see the `glob` man page.

- **interval**
  Specifies, in seconds, the frequency at which the system issues the monitor check when either the resource is **down** or the status of the resource is unknown. The default value is 5 seconds.
◆ **manual-resume**
  Specifies whether the system automatically changes the status of a resource to **up** at the next successful monitor check. The default value of the `manual-resume` option is **disabled**.

  If you set the `manual-resume` option to **enabled**, you must manually mark the resource as **up** before the system can use it for load balancing connections.

◆ **method**
  Displays the GET method. You cannot modify the method. The default value is **none**.

◆ **name**
  Specifies a unique name for the component. This option is required for the commands `create`, `delete`, and `modify`.

◆ **namespace**
  Specifies the name space for the web service you are monitoring, for example: `http://example.com/`. The default value is **none**.

◆ **parameter-name**
  If the method has a parameter, specifies the name of that parameter. The default value is **none**.

◆ **parameter-type**
  Specifies the parameter type. The default value is `bool`.

◆ **parameter-value**
  Specifies the value for the parameter. The default value is **none**.

◆ **partition**
  Displays the administrative partition in which the component resides.

◆ **password**
  Specifies the password if the monitored target requires authentication. The default value is **none**.

◆ **protocol**
  Specifies the protocol that the monitor uses to communicate with the target, **http** or **https**. The default value is **http**.

◆ **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (`@[regular expression]`) to indicate that the identifier is a regular expression. For a description of regular expression syntax, see the `regex` man page.

◆ **return-type**
  Specifies the type for the returned parameter. The default value is `bool`.

◆ **return-value**
  Specifies the value for the returned parameter. The default value is **none**.

◆ **time-until-up**
  Specifies the amount of time, in seconds, after the first successful response before a node is marked **up**. A value of **0** (zero) causes a node to be marked **up** immediately after a valid response is received from the node. The default value is **0** (zero).
timeout
Specifies the number of seconds the target has in which to respond to the monitor request. The default value is 16 seconds.
If the target responds within the set time period, it is considered up. If the target does not respond within the set time period, it is considered down. Also, if the target responds with a RESET packet, the system immediately flags the target as down without waiting for the timeout interval to expire.

up-interval
Specifies, in seconds, the frequency at which the system issues the monitor check when the resource is up. The default value is 0 (zero), which specifies that the system uses the value of the interval option whether the resource is up or down.

Important: F5 Networks recommends that when you configure this option and the interval option, that the value that is greater be a multiple of the lesser value to allow for an even distribution of monitor checks among all monitors.

url-path
Specifies the URL for the web service that you are monitoring, for example: /services/myservice.aspx. The default value is none.

username
Specifies the user name if the monitored target requires authentication. The default value is none.

See also

create, delete, edit, glob, list, modify, regex, show, tmsh
**tcp**

Configures a Transmission Control Protocol (TCP) monitor.

**Module**

ltm monitor

**Syntax**

Configure the **tcp** component within the **ltm monitor** module using the following syntax.

**Create/Modify**

```bash
create tcp [name]
modify tcp [name]
options:
    defaults-from [name]
    description [string]
    destination [ip address][port]
    interval [integer]
    manual-resume [enabled | disabled]
    recv [none | [string] ]
    recv-disable [none | [string] ]
    reverse [enabled | disabled]
    send [none | [string] ]
    time-until-up [integer]
    timeout [integer]
    transparent [disabled | enabled]
    up-interval [integer]
```

```bash
edit tcp [ [ [name] | [glob] | [regex] ] ... ]
options:
    all-properties
    non-default-properties
```

**Display**

```bash
list tcp
list tcp [ [ [name] | [glob] | [regex] ] ... ]
show running-config tcp
show running-config tcp [ [ [name] | [glob] | [regex] ] ... ]
options:
    all-properties
```
Delete

\texttt{delete tcp [name]}

\textbf{Note}

\textit{You cannot delete default monitors.}

Description

You can use the \texttt{tcp} component to configure a custom monitor, or you can use the default TCP monitor that Local Traffic Manager provides.

Examples

Creates a monitor named \texttt{my\_tcp} that inherits properties from the default TCP monitor.

\texttt{create tcp my\_tcp defaults-from tcp}

Displays the properties of all of the TCP monitors:

\texttt{list tcp}

Options

You can use these options with the \texttt{tcp} component:

\begin{itemize}
  \item \textbf{defaults-from}
    Specifies the name of the monitor from which you want your custom monitor to inherit settings. The default value is \texttt{tcp}.
  \item \textbf{description}
    User-defined description.
  \item \textbf{destination}
    Specifies the IP address and service port of the resource that is the destination of this monitor. The default value is \texttt{*:}.
    Possible values are:
    \begin{itemize}
      \item \texttt{*:}
        Specifies that the system marks a pool member \texttt{up} or \texttt{down} based on the response of the server at the IP address and port supplied by the pool member.
    \end{itemize}
\end{itemize}
• *:port
  Specifies that the system marks a pool member up or down based on the response of the server at the IP address supplied by the pool member and the port you specify.

• <IP address>:<port>
  Specifies that the system marks a pool member up or down based on the response of the server at the IP address and port you specify.

• <IP address>:<port> (with the transparent option enabled)
  Specifies that the system performs a health check on the server at the IP address and port you specify, routes the check through the IP address and port supplied by the pool member, and marks the pool member (the gateway) up or down accordingly.

◆ glob
  Displays the items that match the glob expression. For a description of glob expression syntax, see the glob man page.

◆ interval
  Specifies, in seconds, the frequency at which the system issues the monitor check when either the resource is down or the status of the resource is unknown. The default value is 5 seconds.

◆ manual-resume
  Specifies whether the system automatically changes the status of a resource to up at the next successful monitor check. The default value of the manual-resume option is disabled.

  If you set the manual-resume option to enabled, you must manually mark the resource as up before the system can use it for load balancing connections.

◆ name
  Specifies a unique name for the component. This option is required for the commands create, delete, and modify.

◆ partition
  Displays the administrative partition in which the component resides.

◆ recv
  Specifies the text string that the monitor looks for in the returned resource. The default value is none.

  The most common receive expressions contain a text string that is included in an HTML file on your site. The text string can be regular text, HTML tags, or image names. If you do not specify a value for both the send and recv options, the monitor performs a simple service check and connect only.

◆ recv-disable
  Specifies the text string that the monitor looks for in the returned resource. If the text string is matched in the returned resource, the corresponding node or pool member is marked session disabled. The default value is none.

  You specify a recv-disable string in the same way that you specify a recv string.


If you specify a `recv-disable` string, you must also specify a `recv` string. You cannot specify a `recv-disable` string if the `reverse` option is enabled.

- **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an @ sign (@[regular expression]) to indicate that the identifier is a regular expression. For a description of regular expression syntax, see the `regex` man page.

- **reverse**
  Specifies whether the monitor operates in reverse mode. When the monitor is in reverse mode, a successful check marks the monitored object down instead of up. You can use this mode only if you configure both the `send` and `recv` options.
  The default value is disabled, which specifies that the monitor does not operate in reverse mode. The enabled value specifies that the monitor operates in reverse mode.

- **send**
  Specifies the text string that the monitor sends to the target object. The default value is GET /, which retrieves a default HTML file for a web site.
  To retrieve a specific page from a web site, specify a fully-qualified path name, for example: GET /www/company/index.html. Since the string can have special characters, the system requires that the string be enclosed with single quotation marks.
  If this value is null, then a valid connection suffices to determine that the service is up. In this case, the system does not need the `recv` option and ignores the option even if not null.

- **time-until-up**
  Specifies the amount of time, in seconds, after the first successful response before a node is marked up. A value of 0 (zero) causes a node to be marked up immediately after a valid response is received from the node. The default value is 0 (zero).

- **timeout**
  Specifies the number of seconds the target has in which to respond to the monitor request. The default value is 16 seconds.
  If the target responds within the set time period, it is considered up. If the target does not respond within the set time period, it is considered down. Also, if the target responds with a RESET packet, the system immediately flags the target as down without waiting for the timeout interval to expire.

- **transparent**
  Specifies whether the monitor operates in transparent mode. Monitors in transparent mode can monitor pool members through firewalls. The default value is disabled.
◆ up-interval
  Specifies, in seconds, the frequency at which the system issues the monitor check when the resource is up. The default value is 0 (zero), which specifies that the system uses the value of the interval option whether the resource is up or down.

  Important: F5 Networks recommends that when you configure this option and the interval option, that the value that is greater be a multiple of the lesser value to allow for an even distribution of monitor checks among all monitors.

See also

create, delete, edit, glob, list, modify, regex, show, tmsh
**tcp-echo**

Configures a Transmission Control Protocol (TCP) Echo monitor.

**Module**

*ltm monitor*

**Syntax**

Configure the *tcp-echo* component within the *ltm monitor* module using the following syntax.

**Create/Modify**

```
create tcp-echo [name]
modify tcp-echo [name]
options:
  defaults-from [name]
  description [string]
  destination [ip address]
  interval [integer]
  manual-resume [enabled | disabled]
  time-until-up [integer]
  timeout [integer]
  transparent [disabled | enabled]
  up-interval [integer]
```

```
edit tcp-echo [ [ [name] | [glob] | [regex] ] ... ]
options:
  all-properties
  non-default-properties
```

**Display**

```
list tcp-echo
list tcp-echo [ [ [name] | [glob] | [regex] ] ... ]
show running-config tcp-echo
show running-config tcp-echo [ [ [name] | [glob] | [regex] ] ... ]
options:
  all-properties
  non-default-properties
  one-line
  partition
```
Delete

\texttt{delete\ tcp-echo\ [name]}

\textbf{Note}

You cannot delete default monitors.

Description

You can use the \texttt{tcp-echo} component to configure a custom monitor, or you can use the default TCP Echo monitor that Local Traffic Manager provides. This type of monitor checks the status of a resource, using TCP.

Examples

Creates a monitor named \texttt{my\_tcp-echo} that inherits properties from the default TCP Echo monitor.
\begin{verbatim}
create\ tcp-echo\ my\_tcp-echo\ defaults-from\ tcp\_echo
\end{verbatim}

Displays the properties of all of the TCP Echo monitors:
\begin{verbatim}
list\ tcp-echo
\end{verbatim}

Options

You can use these options with the \texttt{tcp-echo} component:

\begin{itemize}
  \item \texttt{defaults-from}
    Specifies the name of the monitor from which you want your custom monitor to inherit settings. The default value is \texttt{tcp\_echo}.
  \item \texttt{description}
    User-defined description.
  \item \texttt{destination}
    Specifies the IP address of the resource that is the destination of this monitor. The default value is *.
    Possible values are:
    \begin{itemize}
      \item *
        Specifies that the system performs a health check on the IP address of the node.
      \item \texttt{<IP address>}
        Specifies that the system performs a health check on the IP address that you specify and marks the associated node \textit{up} or \textit{down} as a result of the response.
    \end{itemize}
\end{itemize}
<IP address> (with the transparent option enabled)

Specifies that the system performs a health check on the IP address that you specify, routes the check through the IP address of the associated node, and marks the IP address of the associated node **up** or **down** accordingly.

- **glob**
  Displays the items that match the glob expression. For a description of glob expression syntax, see the glob man page.

- **interval**
  Specifies, in seconds, the frequency at which the system issues the monitor check when either the resource is **down** or the status of the resource is unknown. The default value is 5 seconds.

- **manual-resume**
  Specifies whether the system automatically changes the status of a resource to **up** at the next successful monitor check. The default value of the manual-resume option is **disabled**.

  If you set the manual-resume option to **enabled**, you must manually mark the resource as **up** before the system can use it for load balancing connections.

- **name**
  Specifies a unique name for the component. This option is required for the commands create, delete, and modify.

- **partition**
  Displays the administrative partition in which the component resides.

- **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. For a description of regular expression syntax, see the regex man page.

- **time-until-up**
  Specifies the amount of time, in seconds, after the first successful response before a node is marked **up**. A value of 0 (zero) causes a node to be marked **up** immediately after a valid response is received from the node. The default value is 0 (zero).

- **timeout**
  Specifies the number of seconds the target has in which to respond to the monitor request. The default value is 16 seconds.

  If the target responds within the set time period, it is considered **up**. If the target does not respond within the set time period, it is considered **down**.

  Also, if the target responds with a RESET packet, the system immediately flags the target as **down** without waiting for the timeout interval to expire.

- **transparent**
  Specifies whether the monitor operates in transparent mode. Monitors in transparent mode can monitor pool members through firewalls. The default value is **disabled**.
◆ up-interval
Specifies, in seconds, the frequency at which the system issues the monitor check when the resource is up. The default value is 0 (zero), which specifies that the system uses the value of the interval option whether the resource is up or down.

Important: F5 Networks recommends that when you configure this option and the interval option, that the value that is greater be a multiple of the lesser value to allow for an even distribution of monitor checks among all monitors.

See also
create, delete, edit, glob, list, modify, regex, show, tmsh
tcp-half-open

Configures a Transmission Control Protocol (TCP) Half Open monitor.

Module

ltm monitor

Syntax

Configure the tcp-half-open component within the ltm monitor module using the following syntax.

Create/Modify

create tcp-half-open [name]
modify tcp-half-open [name]
    options:
        defaults-from [name]
        description [string]
        destination [ip address][port]
        interval [integer]
        manual-resume [enabled | disabled]
        time-until-up [integer]
        timeout [integer]
        transparent [disabled | enabled]
        up-interval [integer]
    edit tcp-half-open [ [ [name] | [glob] | [regex] ] ... ]
        options:
            all-properties
            non-default-properties

Display

list tcp-half-open
list tcp-half-open [ [ [name] | [glob] | [regex] ] ... ]
show running-config tcp-half-open
show running-config tcp-half-open [ [ [name] | [glob] | [regex] ] ... ]
    options:
        all-properties
        non-default-properties
        one-line
        partition
Delete

```
delete tcp-half-open [name]
```

◆ Note

You cannot delete default monitors.

Description

You can use the `tcp-half-open` component to configure a custom monitor, or you can use the default TCP Half Open monitor that Local Traffic Manager provides.

Examples

Creates a monitor named `my_tcp-half-open` that inherits properties from the default TCP Half Open monitor.

```
create tcp-half-open my_tcp-half-open defaults-from tcp_half_open
```

Displays the properties of all of the TCP Half Open monitors:

```
list tcp-half-open
```

Options

You can use these options with the `tcp-half-open` component:

◆ `defaults-from`
  Specifies the name of the monitor from which you want your custom monitor to inherit settings. The default value is `tcp_half_open`.

◆ `description`
  User-defined description.

◆ `destination`
  Specifies the IP address and service port of the resource that is the destination of this monitor. The default value is `*:*`.

  Possible values are:

  - `*:*
    Specifies that the system marks a pool member **up** or **down** based on the response of the server at the IP address and port supplied by the pool member.

  - `*:port`
    Specifies that the system marks a pool member **up** or **down** based on the response of the server at the IP address supplied by the pool member and the port you specify.

  - `<IP address>:<port>`
    Specifies that the system marks a pool member **up** or **down** based on the response of the server at the IP address and port you specify.
itm monitor Module Components

- `<IP address>:<port>` (with the `transparent` option enabled)
  Specifies that the system performs a health check on the server at the IP address and port you specify, routes the check through the IP address and port supplied by the pool member, and marks the pool member (the gateway) up or down accordingly.

- `glob`
  Displays the items that match the `glob` expression. For a description of `glob` expression syntax, see the `glob` man page.

- `interval`
  Specifies, in seconds, the frequency at which the system issues the monitor check when either the resource is down or the status of the resource is unknown. The default value is 5 seconds.

- `manual-resume`
  Specifies whether the system automatically changes the status of a resource to up at the next successful monitor check. The default value of the `manual-resume` option is disabled.
  If you set the `manual-resume` option to enabled, you must manually mark the resource as up before the system can use it for load balancing connections.

- `name`
  Specifies a unique name for the component. This option is required for the commands `create`, `delete`, and `modify`.

- `partition`
  Displays the administrative partition in which the component resides.

- `regex`
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. For a description of regular expression syntax, see the `regex` man page.

- `time-until-up`
  Specifies the amount of time, in seconds, after the first successful response before a node is marked up. A value of 0 (zero) causes a node to be marked up immediately after a valid response is received from the node. The default value is 0 (zero).

- `timeout`
  Specifies the number of seconds the target has in which to respond to the monitor request. The default value is 16 seconds.
  If the target responds within the set time period, it is considered up. If the target does not respond within the set time period, it is considered down. Also, if the target responds with a RESET packet, the system immediately flags the target as down without waiting for the timeout interval to expire.

- `transparent`
  Specifies whether the monitor operates in transparent mode. Monitors in transparent mode can monitor pool members through firewalls. The default value is disabled.
◆ up-interval

Specifies, in seconds, the frequency at which the system issues the monitor check when the resource is up. The default value is 0 (zero), which specifies that the system uses the value of the interval option whether the resource is up or down.

*Important:* F5 Networks recommends that when you configure this option and the interval option, that the value that is greater be a multiple of the lesser value to allow for an even distribution of monitor checks among all monitors.

See also

create, delete, edit, glob, list, modify, regex, show, tmsh
The `udp` command configures a User Datagram Protocol (UDP) monitor.

**Module**

`ltm monitor`

**Syntax**

Configure the `udp` component within the `ltm monitor` module using the following syntax.

**Create/Modify**

```plaintext
create udp [name]
modify udp [name]

options:
  debug [no | yes]
  defaults-from [name]
  description [string]
  destination [ip address][port]
  interval [integer]
  manual-resume [enabled | disabled]
  recv [none | [string] ]
  recv-disable [none | [string] ]
  reverse [enabled | disabled]
  send [none | [string] ]
  time-until-up [integer]
  timeout [integer]
  transparent [disabled | enabled]
  up-interval [integer]

edit udp [ [ [name] | [glob] | [regex] ] ... ]

options:
  all-properties
  non-default-properties
```

**Display**

```plaintext
list udp
list udp [ [ [name] | [glob] | [regex] ] ... ]

show running-config udp
show running-config udp [ [ [name] | [glob] | [regex] ] ... ]

options:
```
Delete

delete udp [name]

◆ Note

You cannot delete default monitors.

Description

You can use the udp component to configure a custom monitor, or you can use the default UDP monitor that Local Traffic Manager provides. This type of monitor verifies the UDP service by attempting to send UDP packets to a pool, pool member, or virtual server and receiving a reply.

Examples

Creates a monitor named my_udp that inherits properties from the default UDP monitors.

create udp my_udp defaults-from udp

Displays the properties of all of the UDP monitors:

list udp

Options

You can use these options with the udp component:

◆ debug

Specifies whether the monitor sends error messages and additional information to a log file created and labeled specifically for this monitor. You can use the log information to help diagnose and troubleshoot unsuccessful health checks. The default value is no.

The options are:

• no

  Specifies that the system does not redirect error messages and additional information related to this monitor.

• yes

  Specifies that the system redirects error messages and additional information to the

  /var/log<monitor_type>_<ip address>..<port>.log file.
defaults-from
Specifies the name of the monitor from which you want your custom monitor to inherit settings. The default value is udp.

description
User-defined description.

destination
Specifies the IP address and service port of the resource that is the destination of this monitor. The default value is *:*.
Possible values are:
- *:*  
  Specifies that the system marks a pool member up or down based on the response of the server at the IP address and port supplied by the pool member.
- *:port  
  Specifies that the system marks a pool member up or down based on the response of the server at the IP address supplied by the pool member and the port you specify.
- <IP address>:<port>  
  Specifies that the system marks a pool member up or down based on the response of the server at the IP address and port you specify.
- <IP address>:<port> (with the transparent option enabled)  
  Specifies that the system performs a health check on the server at the IP address and port you specify, routes the check through the IP address and port supplied by the pool member, and marks the pool member (the gateway) up or down accordingly.

glob
Displays the items that match the glob expression. For a description of glob expression syntax, see the glob man page.

interval
Specifies, in seconds, the frequency at which the system issues the monitor check when either the resource is down or the status of the resource is unknown. The default value is 5 seconds.

manual-resume
Specifies whether the system automatically changes the status of a resource to up at the next successful monitor check. The default value of the manual-resume option is disabled.
If you set the manual-resume option to enabled, you must manually mark the resource as up before the system can use it for load balancing connections.

name
Specifies a unique name for the component. This option is required for the commands create, delete, and modify.

partition
Displays the administrative partition in which the component resides.

test
Specifies the text string that the monitor looks for in the returned resource. The default value is none.
◆ **recv-disable**
Specifies the text string that the monitor looks for in the returned resource. The default value is **none**.

The **recv-disable** string can be specified the same way a **recv** string can be specified.

If the **recv-disable** string is configured, the recv string must be non-empty. The **recv-disable** string cannot be configured if **reverse** mode is enabled.

◆ **regex**
Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. For a description of regular expression syntax, see the **regex** man page.

◆ **reverse**
Specifies whether the monitor operates in reverse mode. When the monitor is in reverse mode, a successful check marks the monitored object **down** instead of **up**. You can use the this mode only if you configure both the **send** and **recv** options.

The default value is **disabled**, which specifies that the monitor does not operate in reverse mode. The **enabled** value specifies that the monitor operates in reverse mode.

◆ **send**
Specifies the text string that the monitor sends to the target object. The default value is **GET /**, which retrieves a default HTML file for a web site.

To retrieve a specific page from a web site, specify a fully-qualified path name, for example: **GET /www/company/index.html**. Since the string can have special characters, the system requires that the string be enclosed with single quotation marks.

If this value is null, then a valid connection suffices to determine that the service is **up**. In this case, the system does not need the value of the **recv** option and ignores the option even if not null.

◆ **time-until-up**
Specifies the amount of time, in seconds, after the first successful response before a node is marked **up**. A value of 0 (zero) causes a node to be marked **up** immediately after a valid response is received from the node. The default value is 0 (zero).

◆ **timeout**
Specifies the number of seconds the target has in which to respond to the monitor request. The default value is 16 seconds.

If the target responds within the set time period, it is considered **up**. If the target does not respond within the set time period, it is considered **down**. Also, if the target responds with a RESET packet, the system immediately flags the target as **down** without waiting for the timeout interval to expire.
◆ **transparent**
  Specifies whether the monitor operates in transparent mode. Monitors in transparent mode can monitor pool members through firewalls. The default value is **disabled**.

◆ **up-interval**
  Specifies, in seconds, the frequency at which the system issues the monitor check when the resource is **up**. The default value is **0** (zero), which specifies that the system uses the value of the **interval** option whether the resource is **up** or **down**.

  **Important:** F5 Networks recommends that when you configure this option and the **interval** option, that the value that is greater be a multiple of the lesser value to allow for an even distribution of monitor checks among all monitors.

### See also

create, delete, edit, glob, list, modify, regex, show, tmsh
virtual-location

Configures a virtual location monitor.

Module

ltm monitor

Syntax

Configure the virtual-location component within the ltm monitor module using the syntax shown in the following sections.

Create/Modify

create virtual-location [name]
modify virtual-location [name]
   options:
      debug [no | yes]
      defaults-from [name]
      description [string]
      interval [integer]
      pool [name]
      time-until-up [integer]
      timeout [integer]
      up-interval [integer]
edit virtual-location [ [ [name] | [glob] | [regex] ] ... ]
   options:
      all-properties
      non-default-properties

Display

list virtual-location
list virtual-location [ [ [name] | [glob] | [regex] ] ... ]
show running-config virtual-location
show running-config virtual-location
   [ [ [name] | [glob] | [regex] ] ... ]
   options:
      all-properties
      non-default-properties
      one-line
      partition
Delete

\texttt{delete virtual-location [name]}

\textbf{Note}

\textit{You cannot delete default monitors.}

Description

The virtual location monitor determines if a pool member that has a virtual IP is currently a local pool member with its arp entry existing on a local VLAN, or, a remote pool member with its ARP entry existing on a tunnel VLAN. If the pool member is local, it sets the pool member’s priority to 2. If the pool member is remote it, will set the priority to 1 (a lower priority). The virtual location always returns up as the availability for the pool member. It is necessary to use an additional monitor to check the availability status of the pool member.

You can use the \texttt{virtual-location} component to configure a custom monitor, or you can use the default virtual location monitor that Local Traffic Manager provides.

Examples

Creates a monitor named \texttt{my\_virtual-location} that inherits properties from the default virtual location monitor.

\texttt{create virtual-location my\_virtual-location defaults-from virtual\_location pool aPool}

Displays the properties of all of the virtual location monitors:

\texttt{list virtual-location}

Options

You can use these options with the \texttt{virtual-location} component:

- \texttt{debug}

  Specifies whether the monitor sends error messages and additional information to a log file created and labeled specifically for this monitor. The default setting is \texttt{no}. You can use the log information to help diagnose and troubleshoot unsuccessful health checks.

  The options are:

  - \texttt{no} (specifies that the system does not redirect error messages and additional information related to this monitor.)

  - \texttt{yes} (specifies that the system redirects error messages and additional information to the \texttt{/var/log<monitor\_type>_<ip\_address>_<port>\.log} file.)
◆ **defaults-from**
  Specifies the name of the monitor from which you want your custom monitor to inherit settings. The default value is `virtual_location`.

◆ **description**
  User-defined description.

◆ **glob**
  Displays the items that match the `glob` expression. See `help glob` for a description of `glob` expression syntax.

◆ **interval**
  Specifies, in seconds, the frequency at which the system issues the monitor check when either the resource is `down` or the status of the resource is unknown. The default value is 5 seconds.

  **Important:** F5 Networks recommends that when you configure this option and the `up-interval` option, whichever value is greater be a multiple of the lesser value to allow for an even distribution of monitor checks among all monitors.

◆ **name**
  Specifies a unique name for the component. This option is required for the commands `create`, `delete`, and `modify`.

◆ **partition**
  Displays the administrative partition in which the component resides.

◆ **pool**
  Specifies the pool for the target pool member. This is a required argument.

◆ **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. See `help regex` for a description of regular expression syntax.

◆ **time-until-up**
  Specifies the amount of time, in seconds, after the first successful response before a node is marked up. A value of 0 (zero) causes a node to be marked up immediately after a valid response is received from the node. The default value is 0 (zero).

◆ **timeout**
  Specifies the number of seconds the target has in which to respond to the monitor request. The default value is 16 seconds.

  If the target responds within the set time period, it is considered up. If the target does not respond within the set time period, it is considered down. Also, if the target responds with a RESET packet, the system immediately flags the target as down without waiting for the timeout interval to expire.

◆ **up-interval**
  Specifies, in seconds, the frequency at which the system issues the monitor check when the resource is up. The default value is 0 (zero), which specifies that the system uses the value of the `interval` option whether the resource is up or down.
Important: F5 Networks recommends that when you configure this option and the interval option, whichever value is greater be a multiple of the lesser value to allow for an even distribution of monitor checks among all monitors.

See also

create, delete, edit, glob, list, ltm pool, modify, regex, tmsh
Chapter 31

wap

Configures a Wireless Application Protocol (WAP) monitor.

Module

ltm monitor

Syntax

Configure the wap component within the ltm monitor module using the following syntax.

Create/Modify

create wap [name]
modify wap [name]
  options:
    accounting-node [none | [RADIUS server name] ]
    accounting-port [ [integer] | none]
    call-id [none | [RADIUS server 11 digit phone number] ]
    debug [no | yes]
    defaults-from [name]
    description [string]
    destination [ip address][port]
    framed-address [none | [RADIUS framed IP address] ]
    interval [integer]
    manual-resume [enabled | disabled]
    recv [none | [string] ]
    secret [none | [password] ]
    send [none | [string] ]
    server-id [none | [RADIUS NAS-ID] ]
    session-id [none | [RADIUS session ID] ]
    time-until-up [integer]
    timeout [integer]
    up-interval [integer]
edit wap [[ [name] | [glob] | [regex] ] ... ]
  options:
    all-properties
    non-default-properties
Display

list wap
list wap [ [ [name] | [glob] | [regex] ] ... ]
show running-config wap
show running-config wap [ [ [name] | [glob] | [regex] ] ... ]

options:
  all-properties
  non-default-properties
  one-line
  partition

Delete

delete wap [name]

◆ Note

You cannot delete default monitors.

Description

You can use the wap component to configure a custom monitor, or you can use the default WAP monitor that Local Traffic Manager provides. This type of monitor requests the URL specified in the send option and finds the string specified in the recv option somewhere in the data returned by the URL response.

Examples

Creates a monitor named my_wap that inherits properties from the default WAP monitor.
create wap my_wap defaults-from wap

Displays the properties of all of the WAP monitors:
list wap

Options

You can use these options with the wap component:

◆ accounting-node
  Specifies the RADIUS server that provides authentication for the WAP target. If you configure the accounting-port option, but you do not configure the this option, the system assumes that the RADIUS server and the WAP server are the same system.
◆ **accounting-port**
   Specifies the port that the monitor uses for RADIUS accounting. The default value is **none**. A value of 0 (zero) disables RADIUS accounting.

◆ **call-id**
   Specifies the 11-digit phone number for the RADIUS server. The default value is **none**.

◆ **debug**
   Specifies whether the monitor sends error messages and additional information to a log file created and labeled specifically for this monitor. You can use the log information to help diagnose and troubleshoot unsuccessful health checks. The default value is **no**.

   The options are:
   - **no**
     Specifies that the system does not redirect error messages and additional information related to this monitor.
   - **yes**
     Specifies that the system redirects error messages and additional information to the 
     /var/log/<monitor_type>_<ip address>_<port>.log file.

◆ **defaults-from**
   Specifies the name of the monitor from which you want your custom monitor to inherit settings. The default value is **wap**.

◆ **description**
   User-defined description.

◆ **destination**
   Specifies the IP address and service port of the resource that is the destination of this monitor. The default value is ***:***.

   Possible values are:
   - ***:***
     Specifies that the system marks a pool member **up** or **down** based on the response of the server at the IP address and port supplied by the pool member.
   - ***:port**
     Specifies that the system marks a pool member **up** or **down** based on the response of the server at the IP address supplied by the pool member and the port you specify.
   - **<IP address>**:<port>**
     Specifies that the system marks a pool member **up** or **down** based on the response of the server at the IP address and port you specify.

◆ **framed-address**
   Specifies the RADIUS framed IP address. The default value is **none**.

◆ **glob**
   Displays the items that match the **glob** expression. For a description of **glob** expression syntax, see the **glob** man page.
◆ **interval**
   Specifies, in seconds, the frequency at which the system issues the monitor check when either the resource is **down** or the status of the resource is unknown. The default value is **10** seconds.

◆ **manual-resume**
   Specifies whether the system automatically changes the status of a resource to **up** at the next successful monitor check. The default value of the **manual-resume** option is **disabled**.
   If you set the **manual-resume** option to **enabled**, you must manually mark the resource as **up** before the system can use it for load balancing connections.

◆ **name**
   Specifies a unique name for the component. This option is required for the commands **create**, **delete**, and **modify**.

◆ **partition**
   Displays the administrative partition in which the component resides.

◆ **recv**
   Specifies the text string that the monitor looks for in the returned resource. The most common receive expressions contain a text string that is included in an HTML file on your site. The text string can be regular text, HTML tags, or image names. If you do not specify both a value for both the **send** and **recv** options, the monitor performs a simple service check and connect only. The default value is **none**.

◆ **regex**
   Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. For a description of regular expression syntax, see the **regex** man page.

◆ **secret**
   Specifies the password the monitor needs to access the resource. The default value is **none**.

◆ **send**
   Specifies the text string that the monitor sends to the target object. The default value is **GET /**, which retrieves a default HTML file for a web site.
   To retrieve a specific page from a web site, specify a fully-qualified path name, for example: **GET /www/company/index.html**. Since the string can have special characters, the system requires that the string be enclosed with single quotation marks.
   If this value is null, then a valid connection suffices to determine that the service is **up**. In this case, the system does not need the **recv** option and ignores the option even if it is not null. The default value is **none**.

◆ **server-id**
   Specifies the RADIUS NAS-ID for this system when configuring a RADIUS server. The default value is **none**.
◆ **session-id**
   Specifies the RADIUS session identification number when configuring a RADIUS server. The default value is **none**.

◆ **time-until-up**
   Specifies the amount of time, in seconds, after the first successful response before a node is marked **up**. A value of **0** (zero) causes a node to be marked **up** immediately after a valid response is received from the node. The default value is **0** (zero).

◆ **timeout**
   Specifies the number of seconds the target has in which to respond to the monitor request. The default value is **31** seconds.

   If the target responds within the set time period, it is considered **up**. If the target does not respond within the set time period, it is considered **down**. Also, if the target responds with a RESET packet, the system immediately flags the target as **down** without waiting for the timeout interval to expire.

◆ **up-interval**
   Specifies, in seconds, the frequency at which the system issues the monitor check when the resource is **up**. The default value is **0** (zero), which specifies that the system uses the value of the **interval** option whether the resource is **up** or **down**.

   **Important:** F5 Networks recommends that when you configure this option and the **interval** option, that the value that is greater be a multiple of the lesser value to allow for an even distribution of monitor checks among all monitors.

---

**See also**

create, delete, edit, glob, list, modify, regex, show, tmsh
wmi

Configures a Windows Management Infrastructure (WMI) monitor.

Module

ltm monitor

Syntax

Configure the wmi component within the ltm monitor module using the following syntax.

Create/Modify

create wmi [name]
modify wmi [name]
  options:
    agent [string]
    command [ [command] | none]
    defaults-from [name]
    description [string]
    interval [integer]
    metrics [ [value] | none]
    password [none | [password] ]
    post [none | [string] ]
    time-until-up [integer]
    timeout [integer]
    url [none | [URL] ]
    username [ [name] | none]
edit wmi [ [ [name] | [glob] | [regex] ] ... ]
  options:
    all-properties
    non-default-properties

Display

list wmi
list wmi [ [ [name] | [glob] | [regex] ] ... ]
show running-config wmi
show running-config wmi [ [ [name] | [glob] | [regex] ] ... ]
  options:
    agent
    all-properties
Chapter 31

method
non-default-properties
one-line
partition
post

Delete

delete wmi [name]

◆ Note

You cannot delete default monitors.

Description

You can use the wmi component to configure a custom monitor, or you can use the default WMI monitor that Local Traffic Manager provides. This type of monitor checks the performance of a pool, pool member, or virtual server that is running the WMI data collection agent, and then dynamically load balances traffic accordingly.

 Examples

Creates a monitor named my_wmi that inherits properties from the default WMI monitor.
create wmi my_wmi defaults-from wmi

Displays the properties of all of the WMI monitors:
list wmi

Options

You can use these options with the wmi component:

◆ agent
  Displays the agent for the monitor. The default agent is Mozilla/4.0 (compatible: MSIE 5.0; Windows NT).

◆ command
  Specifies the command that the system uses to obtain the metrics from the resource. See the documentation for this resource for information on available commands.

◆ defaults-from
  Specifies the name of the monitor from which you want your custom monitor to inherit settings. The default value is wmi.

◆ description
  User-defined description.
itm monitor Module Components

- **glob**
  Displays the items that match the **glob** expression. For a description of **glob** expression syntax, see the **glob** man page.

- **interval**
  Specifies the frequency at which the system issues the monitor check. The default value is 5 seconds.

- **method**
  Displays the GET method. You cannot modify the method.

- **metrics**
  Specifies the performance metrics that the commands collect from the target. The default value is **LoadPercentage**, **DiskUsage**, **PhysicalMemoryUsage:1.5**, **VirtualMemoryUsage:2.0**.

- **name**
  Specifies a unique name for the component. This option is required for the commands **create**, **delete**, and **modify**.

- **partition**
  Displays the administrative partition in which the component resides.

- **password**
  Specifies the password if the monitored target requires authentication. The default value is **none**.

- **post**
  Specifies the mechanism that the monitor uses for posting. The default value is **RespFormat=HTML**. You cannot change the post format for WMI monitors.

- **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. For a description of regular expression syntax, see the **regex** man page.

- **time-until-up**
  Specifies the amount of time, in seconds, after the first successful response before a node is marked **up**. A value of 0 (zero) causes a node to be marked **up** immediately after a valid response is received from the node. The default value is 0 (zero).

- **timeout**
  Specifies the number of seconds the target has in which to respond to the monitor request. The default value is 16 seconds.

  If the target responds within the set time period, it is considered **up**. If the target does not respond within the set time period, it is considered **down**. Also, if the target responds with a RESET packet, the system immediately flags the target as **down** without waiting for the timeout interval to expire.

- **url**
  Specifies the URL that the monitor uses. The default value is **/scripts/f5Isapi.dll**.
• **username**
  Specifies the user name if the monitored target requires authentication.
  The default value is **none**.

**See also**

`create`, `delete`, `edit`, `glob`, `list`, `modify`, `regex`, `show`, `tmsh`
Ltm persistence Module Components

- Introducing the Ltm persistence module
- Alphabetical list of components
Introducing the ltm persistence module

You can use the tmsh components that reside within the ltm persistence module to configure persistence for the BIG-IP® system. For more information about the tmsh hierarchical structure, see Chapter 2, Understanding and Using the Traffic Management Shell.

Alphabetical list of components

The remainder of this chapter lists the tmsh components that are available in the ltm persistence module.
**cookie**

Configures a cookie persistence profile.

**Module**

**ltm persistence**

**Syntax**

Configure the `cookie` component within the `ltm persistence` module using the following syntax.

**Create/Modify**

```
create cookie [name]
modify cookie [name]
```

```
options:
  all
  always-send [enabled | disabled]
  cookie-name [name] | none
  defaults-from [name]
  description [string]
  expiration [d:h:m:s] | [h:m:s] | [m:s] | [seconds] | "session cookie"
  hash-length [integer]
  hash-offset [integer]
  match-across-pools [enabled | disabled]
  match-across-services [enabled | disabled]
  match-across-virtuals [enabled | disabled]
  method [hash | insert | passive | rewrite]
  mirror [enabled | disabled]
  override-connection-limit [enabled | disabled]
  timeout [indefinite | [integer] ]
```

```
edit cookie [ [name] | [glob] | [regex] ] ... ]
```

```
options:
  all-properties
  non-default-properties
```

**Display**

```
list cookie
```

```
list cookie [ [name] | [glob] | [regex] ] ... ]
```

```
show running-config cookie
```

```
show running-config cookie [ [name] | [glob] | [regex] ] ... ]
```
options:
  all
  all-properties
  non-default-properties
  one-line
  partition

Delete

delete cookie [name]
  options:
    all

Description

You can use the cookie component to configure a cookie persistence profile for the BIG-IP system. Cookie persistence uses an HTTP cookie stored on a client’s computer to allow the client to connect to the same server previously visited at a web site.

A persistence profile is a profile that enables persistence when you assign the profile to a virtual server. Using a persistence profile means that you do not have to write an iRule to implement a type of persistence. You can either use the default profile or create a custom profile based on the default.

Examples

Displays all cookie persistence profiles:
list cookie

Creates a custom cookie persistence profile named cookie_persistence that inherits its settings from the default cookie persistence profile:
create cookie cookie_persistence defaults-from cookie

Options

You can use the following options with the cookie component:

- **always-send**
  Send the cookie persistence entry on every reply, even if the entry has previously been supplied to the client. The default value is disabled.

- **cookie-name**
  Specifies a unique name for the cookie. This option is required.

- **defaults-from**
  Specifies the existing profile from which the system imports settings for the new profile. The default value is cookie, the system default cookie persistence profile.
◆ **description**
User-defined description.

◆ **expiration**
Specifies the cookie expiration date in the format **d:h:m:s, h:m:s, m:s, or seconds** (hours 0-23, minutes 0-59, seconds 0-59). The time period must be less than 24856 days.
You can use “**session-cookie**” (0 seconds) to indicate that the cookie expires when the browser closes.

◆ **glob**
Displays the items that match the **glob** expression. For a description of **glob** expression syntax, see the **glob** man page.

◆ **hash-length**
Specifies the cookie hash length. The length is the number of bytes to use when calculating the hash value. The default value is **0** (zero) bytes.

◆ **hash-offset**
Specifies the cookie hash offset. The offset is the number of bytes in the cookie to skip before calculating the hash value. The default value is **0** (zero) bytes.

◆ **match-across-pools**
Specifies, when enabled, that the system can use any pool that contains this persistence record. The default value is **disabled**.

◆ **match-across-services**
Specifies, when enabled, that all persistent connections from a client IP address, which go to the same virtual IP address, also go to the same node. The default value is **disabled**.

◆ **match-across-virtuals**
Specifies, when enabled, that all persistent connections from the same client IP address go to the same node. The default value is **disabled**.

◆ **method**
Specifies the type of cookie processing that the system uses. The default value is **insert**.

◆ **mirror**
Indicates whether the system mirrors persistence records to the high-availability peer. This option is applicable only when the value of the **method** option is **hash**. The default value is **disabled**.

◆ **name**
Specifies a unique name for the component. This option is required for the commands **create**, **delete**, and **modify**.

◆ **override-connection-limit**
When this option is **enabled**, the pool member connection limits are not enforced for persisted clients. Note that connection limits that are set on virtual servers remain hard limits and are not disabled. The default value is **disabled**.

◆ **partition**
Displays the administrative partition within which the component resides.
- **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. For a description of regular expression syntax, see the `regex` man page.

- **timeout**
  Specifies the duration of the persistence entries. The default value is 0 (zero) seconds.

### See also

*create, delete, edit, glob, list, ltm virtual, modify, regex, show, tmsh*
dest-addr

Configures a destination address affinity persistence profile.

Module

ltm persistence

Syntax

Configure the dest-addr component within the ltm persistence module using the following syntax.

Create/Modify

create dest-addr [name]
modify dest-addr [name]
   options:
      all
      defaults-from [name]
      description [string]
      mask [ [ip address] | none]
      match-across-pools [enabled | disabled]
      match-across-services [enabled | disabled]
      match-across-virtuals [enabled | disabled]
      mirror [enabled | disabled]
      override-connection-limit [enabled | disabled]
      timeout [integer]
edit dest-addr [ [ [name] | [glob] | [regex] ] ... ]
   options:
      all-properties
      non-default-properties

Display

list dest-addr
list dest-addr [ [ [name] | [glob] | [regex] ] ... ]
show running-config dest-addr
show running-config dest-addr [ [ [name] | [glob] | [regex] ] ... ]
   options:
      all
      all-properties
      non-default-properties
      one-line
      partition
Delete

\texttt{delete dest-addr [name]}

\texttt{options:}

\texttt{all}

Description

You can use the \texttt{dest-addr} component to configure a destination address affinity persistence profile for the BIG-IP system. Also known as sticky persistence, destination address affinity persistence supports TCP and UDP protocols, and directs session requests to the same server based solely on the destination IP address of a packet.

A \textit{persistence} profile is a profile that enables persistence when you assign the profile to a virtual server. Using a persistence profile means that you do not have to write an iRule to implement a type of persistence. You can either use the default profile or create a custom profile based on the default.

Examples

Displays all destination address affinity persistence profiles:

\texttt{list dest-addr}

Creates a custom destination address affinity persistence profile named \texttt{da_persistence} that inherits its settings from the default destination address affinity persistence profile:

\texttt{create dest-addr da_persistence defaults-from dest-addr}

Options

You can use the following options with the \texttt{dest-addr} component:

\begin{itemize}
  \item \texttt{defaults-from}
    \begin{itemize}
      \item Specifies the existing profile from which the system imports settings for the new profile. The default value is \texttt{dest_addr}, the system default destination address affinity persistence profile.
    \end{itemize}
  \item \texttt{description}
    \begin{itemize}
      \item User-defined description.
    \end{itemize}
  \item \texttt{glob}
    \begin{itemize}
      \item Displays the items that match the \texttt{glob} expression. For a description of \texttt{glob} expression syntax, see the \texttt{glob} man page.
    \end{itemize}
  \item \texttt{mask}
    \begin{itemize}
      \item Specifies an IP mask. This is the mask used by simple persistence for connections. The default value is ::.
    \end{itemize}
\end{itemize}
match-across-pools
Specifies, when enabled, that the system can use any pool that contains this persistence record. The default value is disabled.

match-across-services
Specifies, when enabled, that all persistent connections from a client IP address, which go to the same virtual IP address, also go to the same node. The default value is disabled.

match-across-virtuals
Specifies, when enabled, that all persistent connections from the same client IP address go to the same node. The default value is disabled.

mirror
Indicates whether the system mirrors persistence records to the high-availability peer. The default value is disabled.

name
Specifies a unique name for the component. This option is required for the commands create, delete, and modify.

override-connection-limit
Specifies, when enabled, that the pool member connection limits are not enforced for persisted clients. Note that connection limits that are set on virtual servers remain hard limits and are not disabled. The default value is disabled.

partition
Displays the administrative partition within which the component resides.

regex
Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. For a description of regular expression syntax, see the regex man page.

timeout
Specifies the duration of the persistence entries. The default value is 180 seconds.

See also
create, delete, edit, glob, list, ltm virtual, modify, regex, show, tmsh
**global-settings**

Configures persistence for the BIG-IP system.

**Module**

**ltm persistence**

**Syntax**

Configure the `global-settings` component within the `ltm persistence` module using the following syntax.

**Modify**

```
modify global-settings [option name]
options:
    description [string]
    dest-addr-limit-mode [timeout | maxcount]
    dest-addr-max [integer]
    proxy-group [string]
edit global-settings [ [ [name] | [glob] | [regex] ] ... ]
options:
    all-properties
    non-default-properties
```

**Display**

```
list global-settings
list global-settings [ [ [name] | [glob] | [regex] ] ... ]
show running-config global-settings
show running-config global-settings
    [ [ [name] | [glob] | [regex] ] ... ]
options:
    all-properties
    non-default-properties
    one-line
```

**Description**

You can use the `global-settings` component within the `ltm persistence` module to configure persistence for the system.
For information about configuring session persistence for a virtual server, see the man pages for the following components: `ltm persistence hash`, `ltm persistence msrdp`, `ltm persistence sip`, `ltm persistence source-addr`, `ltm persistence ssl`, and `ltm persistence universal`.

**Examples**

Displays the global persistence configuration:

```bash
list global-settings
```

Sets the value of the option `dest-addr-limit-mode` to `maxcount`, which indicates that a persistence session is limited by the maximum number of requests to the destination address:

```bash
modify global-settings dest-addr-limit-mode maxcount
```

**Options**

You can use the following options with the `global-settings` component:

- **description**
  User-defined description.

- **dest-addr-limit-mode**
  Specifies that a persistence session is limited by either the number of seconds before the persistence entry times out or by a maximum number of requests to the destination address. The default value is `timeout`.

- **dest-addr-max**
  Specifies the maximum number of entries that the persistence table can contain at any one time, when the value of the option `dest-addr-limit-mode` is `maxcount`. The default value is `2048` entries.

- **glob**
  Displays the items that match the `glob` expression. For a description of `glob` expression syntax, see the `glob` man page.

- **proxy-group**
  Specifies a group of servers that are configured to process all of the requests from a single source address during a persistence session. The default value is `aol`.

- **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (`@[regular expression]`) to indicate that the identifier is a regular expression. For a description of regular expression syntax, see the `regex` man page.

**See also**

`edit`, `glob`, `list`, `ltm virtual`, `modify`, `regex`, `show`, `tmsh`
hash

Configures a hash persistence profile.

Module

ltm persistence

Syntax

Configure the hash component within the ltm persistence module using the following syntax.

Create/Modify

create hash [name]
modify hash [name]

options:
  all
  defaults-from [name]
  description [string]
  hash-algorithm [default | carp]
  hash-buffer-limit [integer]
  hash-end-pattern [none | [string] ]
  hash-length [integer]
  hash-offset [integer]
  hash-start-pattern [none | [string] ]
  match-across-pools [enabled | disabled]
  match-across-services [enabled | disabled]
  match-across-virtuals [enabled | disabled]
  mirror [enabled | disabled]
  override-connection-limit [enabled | disabled]
  rule [iRule name]
  timeout [integer]

edit hash [ [ [name] | [glob] | [regex] ] ... ]

options:
  all-properties
  non-default-properties

Display

list hash
list hash [ [ [name] | [glob] | [regex] ] ... ]
show running-config hash
show running-config hash [ [ [name] | [glob] | [regex] ] ... ]
options:
  all
  all-properties
  non-default-properties
  one-line
  partition

Delete
delete hash [name]
options:
  all

Description
You can use the hash component to configure a hash persistence profile for the BIG-IP system. Hash persistence is based on an existing iRule.

A persistence profile is a profile that enables persistence when you assign the profile to a virtual server. Using a persistence profile means that you do not have to write an iRule to implement a type of persistence. You can either use the default profile or create a custom profile based on the default.

Examples
Displays all hash persistence profiles:
list hash

Creates a custom hash persistence profile named hash_persistence that inherits its settings from the default hash persistence profile:
create hash hash_persistence defaults-from hash

Options
You can use the following options with the hash component:

- **defaults-from**
  Specifies the existing profile from which the system imports settings for the new profile. The default value is hash, the system default hash persistence profile.

- **description**
  User-defined description.

- **glob**
  Displays the items that match the glob expression. For a description of glob expression syntax, see the glob man page.
- **hash-algorithm**
  Specifies the algorithm the system uses for hash persistence load balancing. The hash result is the input for the algorithm. The default value is `default`.
  The options are:
  - **carp**
    Uses the Cache Array Routing Protocol (CARP) to obtain the hash result for the input to the algorithm.
  - **default**
    Uses the index of pool members to obtain the hash result for the input to the algorithm.

- **hash-buffer-limit**
  Specifies the maximum buffer length the system collects to locate the hashing pattern for hash persistence load balancing. The default value is 0 (zero).

- **hash-end-pattern**
  Specifies the string that describes the ending location of the hash pattern that the system uses to perform hash persistence load balancing. The default value is `none`.

- **hash-length**
  Specifies the length of data within the packet in bytes that the system uses to calculate the hash value when performing hash persistence load balancing. The default value is 0 (zero) bytes.

- **hash-offset**
  Specifies the start offset within the packet from which the system begins the hash when performing hash persistence load balancing. The default value is 0 (zero).

- **hash-start-pattern**
  Specifies the string that describes the start location of the hash pattern that the system uses to perform hash persistence load balancing. The default value is `none`.

- **match-across-pools**
  Specifies, when enabled, that the system can use any pool that contains this persistence record. The default value is `disabled`.

- **match-across-services**
  Specifies, when enabled, that all persistent connections from a client IP address, which go to the same virtual IP address, also go to the same node. The default value is `disabled`.

- **match-across-virtuals**
  Specifies, when enabled, that all persistent connections from the same client IP address go to the same node. The default value is `disabled`.

- **mirror**
  Indicates whether the system mirrors persistence records to the high-availability peer. The default value is `disabled`.

- **name**
  Specifies a unique name for the component. This option is required for the commands `create`, `delete`, and `modify`. 
◆ **override-connection-limit**
  Specifies, when enabled, that the pool member connection limits are not enforced for persisted clients. Note that connection limits that are set on virtual servers remain hard limits and are not disabled. The default value is disabled.

◆ **partition**
  Displays the administrative partition within which the component resides.

◆ **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. For a description of regular expression syntax, see the regex man page.

◆ **rule**
  Specifies a rule name, if you are using a rule for universal persistence.

◆ **timeout**
  Specifies the duration of the persistence entries. The default value is 180 seconds.

**See also**

create, delete, edit, glob, list, ltm virtual, modify, regex, show, tmsh
msrdp

Configures a Microsoft® Remote Display Protocol (MSRDP) persistence profile.

Module

ltm persistence

Syntax

Configure the msrdp component within the ltm persistence module using the following syntax.

Create/Modify

create msrdp [name]
modify msrdp [name]

options:
  all
  defaults-from [name]
  description [string]
  has-session-dir [no | yes]
  match-across-pools [enabled | disabled]
  match-across-services [enabled | disabled]
  match-across-virtuals [enabled | disabled]
  mirror [enabled | disabled]
  override-connection-limit [enabled | disabled]
  timeout [integer]

edit msrdp [ [ [name] | [glob] | [regex] ] ... ]

options:
  all-properties
  non-default-properties

Display

list msrdp
list msrdp [ [ [name] | [glob] | [regex] ] ... ]
show running-config msrdp
show running-config msrdp [ [ [name] | [glob] | [regex] ] ... ]

options:
  all
  all-properties
  non-default-properties
  one-line
  partition
Delete

```
delete msrdp [name]
options:
  all
```

Description

You can use the `msrdp` component to configure an RDP persistence profile for the BIG-IP system. MSRDP persistence provides an efficient way of load balancing traffic and maintaining persistent sessions between Microsoft Windows® clients and servers that are running the Microsoft Terminal Services. The recommended scenario for enabling the MSRDP persistence feature is to create a load balancing pool that consists of members running Windows .NET Server 2003, Enterprise Edition, or later, where all members belong to a Windows cluster and participate in a Windows session directory.

A persistence profile is a profile that enables persistence when you assign the profile to a virtual server. Using a persistence profile means that you do not have to write an iRule to implement a type of persistence. You can either use the default profile or create a custom profile based on the default.

Examples

Displays all MSRDP persistence profiles:

```
list msrdp
```

Creates a custom MSRDP persistence profile named `msrdp_persistence` that inherits its settings from the default MSRDP persistence profile:

```
create msrdp msrdp_persistence defaults-from msrdp
```

Options

You can use the following options with the `msrdp` component:

- **defaults-from**
  Specifies the existing profile from which the system imports settings for the new profile. The default value is `msrdp`, the system default MSRDP persistence profile.

- **description**
  User-defined description.

- **glob**
  Displays the items that match the `glob` expression. For a description of `glob` expression syntax, see the `glob` man page.

- **has-session-dir**
  Specifies whether the Microsoft Terminal Services are configured with a session directory, so the system does not load balance the initial connection. The default value is `yes`. 
◆ **match-across-pools**
   Specifies, when enabled, that the system can use any pool that contains this persistence record. The default value is **disabled**.

◆ **match-across-services**
   Specifies, when enabled, that all persistent connections from a client IP address, which go to the same virtual IP address, also go to the same node. The default value is **disabled**.

◆ **match-across-virtuials**
   Specifies, when enabled, that all persistent connections from the same client IP address go to the same node. The default value is **disabled**.

◆ **mirror**
   Indicates whether the system mirrors persistence records to the high-availability peer. The default value is **disabled**.

◆ **name**
   Specifies a unique name for the component. This option is required for the commands **create**, **delete**, and **modify**.

◆ **override-connection-limit**
   When this option is **enabled**, the pool member connection limits are not enforced for persisted clients. Note that connection limits that are set on virtual servers remain hard limits and are not disabled. The default value is **disabled**.

◆ **partition**
   Displays the administrative partition within which the component resides.

◆ **regex**
   Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. For a description of regular expression syntax, see the regex man page.

◆ **timeout**
   Specifies the duration of the persistence entries. The default value is **300** seconds.

**See also**

create, delete, edit, glob, list, ltm virtual, modify, regex, show, tmsh
Chapter 32

persist-records

Displays or deletes persistence records.

Module

ltm persistence

Syntax

Configure the persist-records component within the ltm persistence module using the following syntax.

Display

show persist-records

options:
  client-addr [ip address]
  key [string]
  mode [cookie | destination-address | hash | mrdp | sip | source-address | ssl-session-id | universal]
  node-addr [ip address]
  node-port [integer]
  pool [string]
  virtual [string]

Delete

delete persist-records

options:
  client-addr [ip address]
  key [string]
  mode [cookie | destination-address | hash | mrdp | sip | source-address | ssl-session-id | universal]
  node-addr [ip address]
  node-port [integer]
  pool [string]
  virtual [string]

Description

You can use the persist-records component to either display or delete persistence records.
Examples

Displays all persistent connections on the BIG-IP system:

```
show persist-records
```

Deletes all persistent connections that originate from the client IP address, 172.19.255.1:

```
delete persist-records client-addr 172.19.255.1
```

Options

You can use the following options with the `msrdp` component:

- **client-addr**
  Specifies the IP address of the client from which the persistent connections you want to view or delete persist.

- **key**
  Specifies a string that the system is using to persist the connections you want to view or delete.

- **mode**
  Specifies the type of persistence of the connections you want to view or delete.
  The options are:
  - **cookie**
    Cookie persistence uses an HTTP cookie stored on a client’s computer to allow the client to connect to the same server previously visited at a web site.
  - **destination-address**
    Also known as sticky persistence, destination address affinity persistence supports TCP and UDP protocols, and directs session requests to the same server based solely on the destination IP address of a packet.
  - **hash**
    Hash persistence is based on an existing iRule.
  - **msrdp**
    MSRDP persistence provides an efficient way of load balancing traffic and maintaining persistent sessions between Windows clients and servers that are running the Microsoft Terminal Services service. The recommended scenario for enabling the MSRDP persistence feature is to create a load balancing pool that consists of members running Windows .NET Server 2003, Enterprise Edition, or later, where all members belong to a Windows cluster and participate in a Windows session directory.
  - **sip**
    Session Initiation Protocol (SIP) persistence is a type of persistence available for server pools. You can configure SIP persistence for
proxy servers that receive SIP messages sent through UDP. The BIG-IP system currently supports persistence for SIP messages sent through UDP, TCP, or SCTP.

- **source-address**
  Also known as simple persistence, source address affinity persistence supports TCP and UDP protocols, and directs session requests to the same server based solely on the source IP address of a packet. When you specify a source address as the mode of persistence, you must specify an IP address using the `client-addr` option.

- **ssl-session-id**
  SSL persistence is a type of persistence that tracks non-terminated SSL sessions, using the SSL session ID. Even when the client's IP address changes, the system still recognizes the connection as being persistent based on the session ID. The term, *non-terminated SSL sessions*, refers to sessions in which the system does not perform the tasks of SSL certificate authentication and encryption/re-encryption.

- **universal**
  Universal persistence allows you to write an expression that defines what to persist on in a packet. The expression, written using the same expression syntax that you use in iRules®, defines some sequence of bytes to use as a session identifier.

- **node-addr**
  Specifies the IP address of the node with which the client sessions that you want to view or delete remain persistent.

- **node-port**
  Specifies the port number of the node with which the client sessions that you want to view or delete remain persistent.

- **pool**
  Specifies the pool member with which the client sessions that you want to view or delete remain persistent.

- **virtual**
  Specifies the virtual server with which the client sessions that you want to view or delete remain persistent.

**See also**

delte, show, tmsh
**sip**

Configures a Session Initiation Protocol (SIP) persistence profile.

**Module**

**ltm persistence**

**Syntax**

Configure the `sip` component within the `ltm persistence` module using the following syntax.

**Create/Modify**

```
create sip [name]
modify sip [name]
   options:
     all
     defaults-from [name]
     description [string]
     match-across-pools [enabled | disabled]
     match-across-services [enabled | disabled]
     match-across-virtuals [enabled | disabled]
     mirror [enabled | disabled]
     override-connection-limit [enabled | disabled]
     sip-info [Call-ID | From | none | SIP-ETag | Subject | To]
     timeout [integer]
```

```
binding string
```

```
edit sip [ [ [name] | [glob] | [regex] ] ... ]
   options:
     all-properties
     non-default-properties
```

**Display**

```
list sip
list sip [ [name] | [glob] | [regex] ] ...
show running-config sip
show running-config sip [ [name] | [glob] | [regex] ] ...
   options:
     all
     all-properties
     non-default-properties
     one-line
     partition
```
Delete

delete sip [name]
options:
  all

Description

You can use the `sip` component to configure a Session Initiation Protocol (SIP) persistence profile for the BIG-IP system. **SIP persistence** is a type of persistence available for server pools. You can configure SIP persistence for proxy servers that receive SIP messages sent through UDP. The BIG-IP system currently supports persistence for SIP messages sent through UDP, TCP, or SCTP.

A **persistence** profile is a profile that enables persistence when you assign the profile to a virtual server. Using a persistence profile means that you do not have to write an iRule to implement a type of persistence. You can either use the default profile or create a custom profile based on the default.

Examples

Displays all SIP persistence profiles:

```
list sip
```

Creates a custom SIP persistence profile named **sip_persistence** that inherits its settings from the default SIP persistence profile:

```
create sip sip_persistence defaults-from sip_info
```

Options

You can use the following options with the `sip` component:

- **defaults-from**
  Specifies the existing profile from which the system imports settings for the new profile. The default value is `sip_info`, the system default SIP persistence profile.

- **description**
  User-defined description.

- **glob**
  Displays the items that match the `glob` expression. For a description of `glob` expression syntax, see the `glob` man page.

- **match-across-pools**
  Specifies, when enabled, that the system can use any pool that contains this persistence record. The default value is `disabled`. 
itm persistence Module Components

- **match-across-services**
  Specifies, when enabled, that all persistent connections from a client IP address, which go to the same virtual IP address, also go to the same node. The default value is **disabled**.

- **match-across-virtuals**
  Specifies, when enabled, that all persistent connections from the same client IP address go to the same node. The default value is **disabled**.

- **mirror**
  Indicates whether the system mirrors persistence records to the high-availability peer. The default value is **disabled**.

- **name**
  Specifies a unique name for the component. This option is required for the commands **create**, **delete**, and **modify**.

- **override-connection-limit**
  When this option is **enabled**, the pool member connection limits are not enforced for persisted clients. Note that connection limits that are set on virtual servers remain hard limits and are not disabled. The default value is **disabled**.

- **partition**
  Displays the administrative partition within which the component resides.

- **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. For a description of regular expression syntax, see the **regex** man page.

- **sip-info**
  Specifies the SIP header field on which you want SIP sessions to persist. The default value is **none**.

- **timeout**
  Specifies the duration of the persistence entries. The default value is **180** seconds.

**See also**

**create**, **delete**, **edit**, **glob**, **list**, **itm virtual**, **modify**, **regex**, **show**, **tmsh**
source-addr

Configures a source address affinity (simple) persistence profile.

Module

ltm persistence

Syntax

Configure the source-addr component within the ltm persistence module using the following syntax.

Create/Modify

create source-addr [name]
modify source-addr [name]

options:
  all
  defaults-from [name]
  description [string]
  map-proxies [enabled | disabled]
  map-proxy-address [ip address]
  map-proxy-class [class name]
  hash-algorithm [carp | default]
  mask [ [ip address] | none]
  match-across-pools [enabled | disabled]
  match-across-services [enabled | disabled]
  match-across-virtuals [enabled | disabled]
  mirror [enabled | disabled]
  override-connection-limit [enabled | disabled]
  timeout [integer]
edit source-addr [ [ [name] | [glob] | [regex] ] ... ]

options:
  all-properties
  non-default-properties

Display

list source-addr
list source-addr [ [ [name] | [glob] | [regex] ] ... ]
show running-config source-addr
show running-config source-addr [ [ [name] | [glob] | [regex] ] ... ]

options:
all
all-properties
non-default-properties
one-line
partition

Delete

dele source-addr [name]
options:
  all

Description

You can use the source-addr component to configure a simple persistence profile for the BIG-IP system. Also known as simple persistence, source address affinity persistence supports TCP and UDP protocols, and directs session requests to the same server based solely on the source IP address of a packet.

A persistence profile is a profile that enables persistence when you assign the profile to a virtual server. Using a persistence profile means that you do not have to write an iRule to implement a type of persistence. You can either use the default profile or create a custom profile based on the default.

Examples

Displays all simple persistence profiles:
list source-addr

Creates a custom simple persistence profile named simple_persistence that inherits its settings from the default simple persistence profile:
create source-addr simple_persistence defaults-from source_addr

Options

You can use the following options with the source-addr component:

- defaults-from
  Specifies the existing profile from which the system imports settings for the new profile. The default value is source_addr, the system default simple persistence profile.

- description
  User-defined description.

- glob
  Displays the items that match the glob expression. For a description of glob expression syntax, see the glob man page.
◆ **map-proxies**
   Enables or disables the map proxies attribute. The default value is **disabled**.

   This attribute controls whether a source address will first be checked against an IP data-group/class to determine whether it is a well-known proxy address. If it matches the IP class, then the source address will be mapped to a single IP address for the purposes of persistence. The default well known proxy class is based on a pre-defined data-group **aol** which represents AOL’s previously published list of proxies. Using this feature enables you to use client/source IP address persistence with a simple persist mask, but forces all clients matching the IP class to persist to the same server. The IP data-group/class can also be changed using either the map-proxy-class profile attribute or globally by changing the DB variable Persist.WellKnownProxyClass. Also, the IP address used for mapping a single source IP address for persistence can also be specifically set using the map-proxy-address profile attribute.

◆ **map-proxy-address**
   Specifies the single IP address to use when the source address matches the proxy data-group/class. The default value is **any** which results in the default behavior of using one of the IP addresses from the proxy data-group/class.

   *Note: This mapped IP address does not have to be contained in the IP data-group/class. It can actually be any IP address since it is only used for keying the persistence record.*

◆ **map-proxy-class**
   Specifies the data-group/class to use for determining whether a source address is from a proxy. The default value is **none** which will result in **map_proxies** using the class defined by the DB variable Persist.WellKnownProxyClass.

◆ **mask**
   Specifies an IP mask. This is the mask used by simple persistence for connections. The default value is **::**.

◆ **match-across-pools**
   Specifies, when enabled, that the system can use any pool that contains this persistence record. The default value is **disabled**.

◆ **match-across-services**
   Specifies, when enabled, that all persistent connections from a client IP address, which go to the same virtual IP address, also go to the same node. The default value is **disabled**.

◆ **match-across-virtuals**
   Specifies, when enabled, that all persistent connections from the same client IP address go to the same node. The default value is **disabled**.

◆ **mirror**
   Indicates whether the system mirrors persistence records to the high-availability peer. The default value is **disabled**.

◆ **name**
   Specifies a unique name for the component. This option is required for the commands **create**, **delete**, and **modify**.
◆ **override-connection-limit**
   When this option is **enabled**, the pool member connection limits are not enforced for persisted clients. Note that connection limits that are set on virtual servers remain hard limits and are not disabled. The default value is **disabled**.

◆ **partition**
   Displays the administrative partition within which the component resides.

◆ **regex**
   Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. For a description of regular expression syntax, see the regex man page.

◆ **timeout**
   Specifies the duration of the persistence entries. The default value is **180** seconds.

See also

create, delete, edit, glob, list, ltm virtual, modify, regex, show, tmsh
Chapter 32

**ssl**

Configures a Secure Socket Layer (SSL) persistence profile.

**Module**

*ltm persistence*

**Syntax**

Configure the **ssl** component within the **ltm persistence** module using the following syntax:

**Create/Modify**

```plaintext
create ssl [name]
modify ssl [name]
  options:
    all
    defaults-from [name]
    description [string]
    match-across-pools [enabled | disabled]
    match-across-services [enabled | disabled]
    match-across-virtuals [enabled | disabled]
    mirror [enabled | disabled]
    override-connection-limit [enabled | disabled]
    timeout [integer]

edit ssl [ [ [name] | [glob] | [regex] ] ... ]
  options:
    all-properties
    non-default-properties
```

**Display**

```plaintext
list ssl
list ssl [ [ [name] | [glob] | [regex] ] ... ]
show running-config ssl
show running-config ssl [ [ [name] | [glob] | [regex] ] ... ]
  options:
    all-properties
    non-default-properties
    one-line
    partition
```
Delete

delete ssl [name]

Description

You can use the ssl component to configure an SSL persistence profile for the BIG-IP system. SSL persistence is a type of persistence that tracks non-terminated SSL sessions, using the SSL session ID. Even when the client's IP address changes, the system still recognizes the connection as being persistent based on the session ID. The term, non-terminated SSL sessions, refers to sessions in which the system does not perform the tasks of SSL certificate authentication and encryption/re-encryption.

A persistence profile is a profile that enables persistence when you assign the profile to a virtual server. Using a persistence profile means that you do not have to write an iRule to implement a type of persistence. You can either use the default profile or create a custom profile based on the default.

Examples

Displays all SSL persistence profiles:

list ssl

Creates a custom SSL persistence profile named ssl_persistence that inherits its settings from the default SSL persistence profile:

create ssl ssl_persistence defaults-from ssl

Options

You can use the following options with the ssl component:

- **defaults-from**
  Specifies the existing profile from which the system imports settings for the new profile. The default value is ssl.

- **glob**
  Displays the items that match the glob expression. For a description of glob expression syntax, see the glob man page.

- **match-across-pools**
  Specifies, when enabled, that the system can use any pool that contains this persistence record. The default value is disabled.

- **match-across-services**
  Specifies, when enabled, that all persistent connections from a client IP address, which go to the same virtual IP address, also go to the same node. The default value is disabled.

- **match-across-virtuals**
  Specifies, when enabled, that all persistent connections from the same client IP address go to the same node. The default value is disabled.
◆ **mirror**
Indicates whether the system mirrors persistence records to the high-availability peer. The default value is **disabled**.

◆ **name**
Specifies a unique name for the component. This option is required for the commands **create**, **delete**, and **modify**.

◆ **override-connection-limit**
When this option is **enabled**, the pool member connection limits are not enforced for persisted clients. Note that connection limits that are set on virtual servers remain hard limits and are not disabled. The default value is **disabled**.

◆ **partition**
Displays the administrative partition within which the component resides.

◆ **regex**
Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. For a description of regular expression syntax, see the regex man page.

◆ **timeout**
Specifies the duration of the persistence entries. The default value is **300** seconds.

**See also**

create, delete, edit, glob, list, ltm virtual, modify, regex, show, tmsh
universal

Configures a universal persistence profile.

Module

ltm persistence

Syntax

Configure the universal component within the ltm persistence module using the following syntax.

Create/Modify

create universal [name]
modify universal [name]
options:
    defaults-from [name]
    description [string]
    match-across-pools [enabled | disabled]
    match-across-services [enabled | disabled]
    match-across-virtuals [enabled | disabled]
    method [hash | insert | passive | rewrite]
    mirror [enabled | disabled]
    override-connection-limit [enabled | disabled]
    rule [ [iRule name] | none]
    timeout [integer]
edit universal [ [name] | [glob] | [regex] ] ... }
options:
    all-properties
    non-default-properties

Display

list universal
list universal [ [name] | [glob] | [regex] ] ... }
show running-config universal
show running-config universal [ [name] | [glob] | [regex] ] ... }
options:
    all-properties
    non-default-properties
    one-line
    partition
Delete

```plaintext
delete universal [name]
  options:
    all
```

Description

You can use the `universal` component to configure a persistence profile for the BIG-IP system. With universal persistence you can write an expression that defines what to persist on in a packet. The expression, written using the same expression syntax that you use in iRules, defines some sequence of bytes to use as a session identifier.

A `persistence` profile is a profile that enables persistence when you assign the profile to a virtual server. Using a persistence profile means that you do not have to write an iRule to implement a type of persistence. You can either use the default profile or create a custom profile based on the default.

Examples

Displays all universal persistence profiles:

```plaintext
list universal
```

Creates a custom universal persistence profile named `uni_persistence` that inherits its settings from the default universal persistence profile:

```plaintext
create universal uni_persistence defaults-from universal
```

Options

You can use the following options with the `universal` component:

- **defaults-from**
  Specifies the existing profile from which the system imports settings for the new profile. The default value is `universal`.

- **description**
  User-defined description.

- **glob**
  Displays the items that match the `glob` expression. For a description of `glob` expression syntax, see the `glob` man page.

- **match-across-pools**
  Specifies, when enabled, that the system can use any pool that contains this persistence record. The default value is `disabled`.

- **match-across-services**
  Specifies, when enabled, that all persistent connections from a client IP address, which go to the same virtual IP address, also go to the same node. The default value is `disabled`.
◆ **match-across-virtuals**
   Specifies, when enabled, that all persistent connections from the same client IP address go to the same node. The default value is **disabled**.

◆ **mirror**
   Indicates whether the system mirrors persistence records to the high-availability peer. The default value is **disabled**.

◆ **name**
   Specifies a unique name for the component. This option is required for the commands **create**, **delete**, and **modify**.

◆ **override-connection-limit**
   When this option is **enabled**, the pool member connection limits are not enforced for persisted clients. Note that connection limits that are set on virtual servers remain hard limits and are not disabled. The default value is **disabled**.

◆ **partition**
   Displays the administrative partition within which the component resides.

◆ **regex**
   Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. For a description of regular expression syntax, see the **regex** man page.

◆ **rule**
   Specifies an iRule name when you are using a rule for universal persistence.

◆ **timeout**
   Specifies the duration of the persistence entries. The default value is **180** seconds.

**See also**

create, delete, edit, glob, list, ltm virtual, modify, regex, show, tmsh
Itm profile Module Components

- Introducing the Itm profile module
- Alphabetical list of components
Introducing the ltm profile module

You can use the tmsh components that reside within the ltm profile module to configure profiles for Local Traffic Manager™. For more information about the tmsh hierarchical structure, see Chapter 2, Understanding and Using the Traffic Management Shell.

Alphabetical list of components

The remainder of this chapter lists the tmsh components that are available in the ltm profile module.
analytics

Configures an analytics profile.

Module

ltm profile

Syntax

Configure the analytics component within the ltm profile module using the syntax shown in the following sections.

Create/Modify

create analytics [name]
modify analytics [name]

options:
  alerts [none | add | delete | modify | replace-all-with] {
    name [string] {
      options:
        granularity [application | pool-member | virtual-server]
        metric [average-page-load-time | average-response-throughput | average-tps |
           max-request-throughput | max-server-latency | average-request-throughput |
           average-server-latency | max-page-load-time | max-response-throughput |
           max-tps]
        sample-period [integer]
        threshold [integer]
        threshold-relation [above | below]
    }
}
captured-traffic-external-logging [enabled | disabled]
captured-traffic-internal-logging [enabled | disabled]
collect-page-load-time [enabled | disabled]
collect-geo [enabled | disabled]
collect-http-throughput [enabled | disabled]
collect-ip [enabled | disabled]
collect-methods [enabled | disabled]
collect-response-codes [enabled | disabled]
collect-server-latency [enabled | disabled]
collect-url [enabled | disabled]
collect-user-agent [enabled | disabled]
collect-user-sessions [enabled | disabled]
collected-stats-external-logging [enabled | disabled]
collected-stats-internal-logging [enabled | disabled]
defaults-from [ analytics profile name [string] | none]
negotiation-by-email [enabled | disabled]
negotiation-by-snmp [enabled | disabled]
negotiation-by-syslog [enabled | disabled]
negotiation-email-addresses [none | add | delete | modify | replace-all-with] {
  email-address [string] }
remote-server-ip [ipv4.address]
remote-server-port [ipv4.port]
remote-server-syslog-facility [local0 | local1 | local2 | local3 | local4 | local5 | local6 | local7]
session-timeout [integer]
smtp-config [ smtp configuration object name ]
traffic-capture [none | add | delete | modify | replace-all-with] { name [string] {
  options:
    captured-protocols [all | http | https]
    virtual-servers [none | add | delete | modify | replace-all-with] { virtual }
    node-addresses [none | add | delete | modify | replace-all-with] { node }
    client-ips [none | add | delete | modify | replace-all-with] { ipv4.address }
    methods [none | add | delete | modify | replace-all-with] { method [string] }
    request-captured-parts [all | body | headers | none]
    request-content-filter-search-part [all | body | headers | none | uri]
    request-content-filter-search-string [none | [string]]
    response-captured-parts [all | body | headers | none]
    response-content-filter-search-part [all | body | headers | none]
    response-content-filter-search-string [none | [string]]
    request-content-filter-search-part [all | body | headers | none]
    request-content-filter-search-string [none | [string]]
    url-path-prefixes [none | add | delete | modify | replace-all-with] {
      url-path-prefix [string] }
    user-agent-substrings [none | add | delete | modify | replace-all-with] {
      user-agent-substring [string] }
  }
}
trust-xff [enabled | disabled]
edit analytics [ [ name ] | [ glob ] | [ regex ] ] ...
  options:
    all-properties
    non-default-properties

Display
list analytics
list analytics [ [ name ] | [ glob ] | [ regex ] ] ...
show running-config analytics
show running-config analytics [ [ name ] | [ glob ] | [ regex ] ] ...
  options:
Delete

delete analytics [name]

Description

Use the analytics component to create, modify, display, or delete an analytics profile for use with analytics functionality.

Examples

Creates a custom analytics profile named my_analytics_profile that inherits its settings from the system default analytics profile:

create analytics my_analytics_profile defaults-from analytics

Displays the properties of all analytics profiles:

list analytics

Options

You can use these options with the analytics component:

- alerts
  Adds, deletes, or replaces a set of analytics alerts. You can configure the following options for an analytics alert:
  - granularity
    Specifies a granularity level on which the alert is defined.
    The options are:
    - application
      Specifies that an alert is triggered for applications for which a threshold is breached.
    - pool-member
      Specifies that an alert is triggered for pool members for which a threshold is breached.
    - virtual-server
      Specifies that an alert is triggered for virtual servers for which a threshold is breached.
• **metric**
  Specifies a metric on which the alert is defined.
  The options are:
  • **average-page-load-time**
    Specifies that an alert is triggered when the average time it takes for the client to respond to a request breaches the defined threshold.
  • **average-request-throughput**
    Specifies that an alert is triggered when the average number of bits per second the system processed, based on requests only, breaches the defined threshold.
  • **average-response-throughput**
    Specifies that an alert is triggered when the average number of bits per second the system processed, based on responses only, breaches the defined threshold.
  • **average-server-latency**
    Specifies that an alert is triggered when the average time it takes for the web server to respond to a request breaches the defined threshold.
  • **average-tps**
    Specifies that an alert is triggered when the average number of transactions per second breaches the defined threshold.
  • **max-page-load-time**
    Specifies that an alert is triggered when the longest time it takes for the client to respond to a request breaches the defined threshold.
  • **max-request-throughput**
    Specifies that an alert is triggered when the maximum number of bits per second the system processed, based on requests only, breaches the defined threshold.
  • **max-response-throughput**
    Specifies that an alert is triggered when the maximum number of bits per second the system processed, based on responses only, breaches the defined threshold.
  • **max-server-latency**
    Specifies that an alert is triggered when the longest time it takes for the web server to respond to a request breaches the defined threshold.
  • **max-tps**
    Specifies that an alert is triggered when the largest number of transactions per second breaches the defined threshold.
  • **name**
    Specifies a unique name for an alert. This option is required for the commands *create*, *delete*, and *modify*.
  • **sample-period**
    Specifies that the alert metric is triggered when the conditions that trigger the alert last a defined amount of time, measured in seconds. The default value is 300.
• **threshold**
  Specifies the threshold that must be breached in order for the system to generate alert.

• **threshold-relation**
  Specifies whether the metric value must be below or above the metric.
  The options are:
  • **above**
    Specifies that an alert is issued if metric current value is above the threshold.
  • **below**
    Specifies that an alert is issued if metric current value is below the threshold.

◆ **captured-traffic-external-logging**
  Enables or disables the external logging of captured traffic.

◆ **captured-traffic-internal-logging**
  Enables or disables the internal logging of captured traffic.

◆ **collect-page-load-time**
  Enables or disables the collection of the page load time statistics. The page load time is the round-trip latency between client end-users and the servers, that is, the round-trip time between an end-user’s request for a page until the time the response finishes loading.

◆ **collect-geo**
  Enables or disables the collection of the names of the countries from where the traffic was sent.

◆ **collect-http-throughput**
  Enables or disables the collection of throughput statistics.

◆ **collect-ip**
  Enables or disables the collection of client IPs statistics.

◆ **collect-methods**
  Enables or disables the collection of HTTP methods statistics.

◆ **collect-response-codes**
  Enables or disables the collection of response codes returned by the servers.

◆ **collect-server-latency**
  Enables or disables the collection of server latency statistics.

◆ **collect-url**
  Enables or disables the collection of requested URL statistics.

◆ **collect-user-agent**
  Enables or disables the collection of user agents.

◆ **collect-user-sessions**
  Enables or disables the collection of the unique user sessions.

◆ **collected-stats-external-logging**
  Enables or disables the external logging of the collected statistics.
- **collected-stats-internal-logging**
  Enables or disables the internal logging of the collected statistics.

- **defaults-from**
  Specifies the profile that you want to use as the parent profile. Your new profile inherits all settings and values from the parent profile specified. The default value is `analytics`.

- **description**
  User-defined description.

- **glob**
  Displays the items that match the `glob` expression. See `help glob` for a description of `glob` expression syntax.

- **name**
  Specifies a unique name for the component. This option is required for the commands `create`, `delete`, and `modify`.

- **notification-by-email**
  Enables or disables sending the analytics alerts by email.

- **notification-by-snmp**
  Enables or disables sending the analytics alerts by SNMP traps. `notification-by-syslog` must be enabled.

- **notification-by-syslog**
  Enables or disables logging of the analytics alerts into the Syslog.

- **notification-email-addresses**
  Specifies which email addresses receive alerts by email when `notification-by-email` is enabled.

- **partition**
  Displays the administrative partition within which the component resides.

- **remote-server-ip**
  Specifies the IP address of a remote server to which the Syslog sends messages.

- **remote-server-port**
  Specifies the port number of a remote server to which the Syslog sends messages. The default value is `514`.

- **remote-server-syslog-facility**
  Specifies the port number of a remote server to which the Syslog sends messages. The default value is `local0`.

- **sampling -ratio**
  Specifies that every `sampling-ratio` transaction is sampled. This attribute can be set in the default profile only. The default value is `1`.

- **session-timeout-minutes**
  Specifies the number of minutes of user non-activity before the system considers the session to be over.

- **smtp-config**
  Specifies the SMTP configuration to be used with analytics.
traffic-capture
Adds, deletes, or replaces an analytics traffic capture definition. You can configure the following options for an analytics traffic capture:

- captured-protocols
  Specifies whether the system captures traffic data sent using all protocols, or only one type of protocol.
  The options are:
  - all
    Specifies that the system captures traffic data sent using all protocols.
  - http
    Specifies that the system captures traffic data sent using http protocol.
  - https
    Specifies that the system captures traffic data sent using https protocol.

- client-ips
  Adds, deletes, or replaces a set of client IP addresses from or to which captured traffic is sent.

- methods
  Adds, deletes, or replaces a set of HTTP methods used to send requests from which traffic is captured.

- name
  Specifies a unique name for an analytics traffic capture. This option is required for the commands create, delete, and modify.

- node-addresses
  Adds, deletes, or replaces a set of node addresses from or to which captured traffic is sent.

- request-captured-parts
  Specifies what parts of the request data the system captures.
  The options are:
  - all
    Specifies that the system captures all the parts of the request data.
  - body
    Specifies that the system captures the body of the request data.
  - headers
    Specifies that the system captures the HTTP headers of the request data.
  - none
    Specifies that the system does not capture the request data.

- request-content-filter-search-part
  Specifies which part of the request is filtered by a specific string.
  The options are:
  - all
    Specifies that the system filters all the parts of the request data.
• **body**  
  Specifies that the system filters the body of the request data.

• **headers**  
  Specifies that the system filters the HTTP headers of the request data.

• **none**  
  Specifies that system does not filter the request data.

• **uri**  
  Specifies that the system filters the URI path component, including the query string, of the request data.

• **request-content-filter-search-string**  
  Specifies the string by which a request data is filtered, or **none**.

• **response-captured-parts**  
  Specifies what parts of the response data the system captures.  
  The options are:

  • **all**  
    Specifies that the system captures all the parts of the response data.

  • **body**  
    Specifies that the system captures the body of the response data.

  • **headers**  
    Specifies that the system captures the HTTP headers of the response data.

  • **none**  
    Specifies that system does not capture the response data.

• **response-codes**  
  Adds, deletes, or replaces a set of HTTP response codes from which traffic is captured.

• **response-content-filter-search-part**  
  Specifies which part of the response is filtered by a specific string.  
  The options are:

  • **all**  
    Specifies that the system filters all the parts of the response data.

  • **body**  
    Specifies that the system filters the body of the response data.

  • **headers**  
    Specifies that the system filters the HTTP headers of the response data.

  • **none**  
    Specifies that system does not filter the response data.

• **response-content-filter-search-string**  
  Specifies the string by which the response data is filtered, or **none**.

• **url-path-prefixes**  
  Adds, deletes, or replaces a set of URL path prefixes on which traffic can be captured (both to and from).
• **user-agent-substrings**
  Adds, deletes, or replaces a set of user agent substrings on which traffic can be captured (both to and from).

• **virtual-servers**
  Adds, deletes, or replaces a set of virtual servers from or to which captured traffic is sent.

• **trust-xff**
  Enables or disables the collection of the client IP address, and statistics from the client IP address, based on the requests XFF (X-forwarded-for) headers, if they exist.

**See also**

create, delete, edit, glob, list, ltm virtual, modify, regex, reset-stats, show, sys smtp, tmsh
certificate-authority

Defines the settings necessary to authenticate the client certificate.

Module

ltm profile

Syntax

Configures the certificate-authority profile within the ltm profile module using the syntax shown in the following sections.

Modify

```
modify certificate-authority [name]
  options:
    authenticate-depth
    ca-file
    crl-file
    default-name
    description
    update-crl
```

```
edit certificate-authority [ [ [name] | [glob] | [regex] ] ... ]
  options:
    all-properties
    non-default-properties
```

Display

```
list certificate-authority
list certificate-authority [ [ [name] | [glob] | [regex] ] ... ]
  app-service
  partition
show certificate-authority
show certificate-authority [ [ [name] | [glob] | [regex] ] ... ]
  options:
    all-properties
    field-fmt
    non-default-properties
    one-line
```
Description

Use the `certificate-authority` component to modify or display a certificate-authority profile.

Examples

Creates a certificate authority profile named mycaprofile using the system defaults:

```plaintext
create ltm profile certificate-authority mycaprofile { ca-file ca.crt }
```

Options

- **app-service**
  Displays the application service to which the object belongs. The default value is `none`.
  
  **Note:** If the strict-updates option is enabled on the Application Service that owns the object, you cannot modify or delete the object. Only the Application Service can modify or delete the object.

- **authenticate-depth**
  Specifies the authenticate depth. This is the client certificate chain maximum traversal depth.

- **ca-file**
  Specifies the certificate authority file name or, you can use `default` for the default certificate authority file name. Configures certificate verification by specifying a list of client or server certificate authorities that the traffic management system trusts.

- **crl-file**
  Specifies the certificate revocation list file name. You can use `default` for the default certificate revocation file name.

- **default-name**
  Specifies the profile that you want to use as the parent profile. Your new profile inherits all settings and values from the parent profile specified.

- **description**
  User-defined description.

- **name**
  Specifies the profile instance name. This option is required for the command `modify`.

- **partition**
  Specifies the administrative partition within which the profile resides.

- **regex**
  Specifies the items that match the regular expression. The regular expression must be preceded by an at sign (`@[regular expression]`) to indicate that the identifier is a regular expression. See `help regex` for a description of regular expression syntax.
◆ **update-crl**
   Automatically updates the CRL file.

**See Also**

edit, glob, list, ltm virtual, modify, regex, reset-stats, show, tmsh, sys smtp-server
Chapter 33

classification

Configures a classification profile.

Module

ltm profile

Syntax

Configures the classification profile within the ltm profile module using the syntax shown in the following sections.

Modify

modify classification [name]

options:
  categories [none | add | delete | replace-all-with] {
    name [string]
  }
  description [string]
  smtp-server [ smtp server configuration object name ]

edit classification [ [ [name] | [glob] | [regex] ] ... ]

options:
  all-properties
  non-default-properties

Display

list classification

list classification [ [ [name] | [glob] | [regex] ] ... ]

show running-config classification

show running-config classification [ [ [name] | [glob] | [regex] ] ... ]

options:
  all-properties
  non-default-properties
  one-line
  partition

Description

Use the classification component to modify, or display a classification profile.
Examples

Edits the classification profile named classification:

```plaintext
edit classification classification
```

◆ **Note**

*The profile name cannot be changed.*

Displays the properties of the classification profile:

```plaintext
list classification
```

Options

◆ **categories**

Adds, deletes, or replaces a set of classification categories. You can configure the following categories: `audio`, `ddl`, `encrypted`, `ftp`, `mail`, `messaging`, `network`, `p2p`, `video`, `video-conf`, `voip`, and `web`.

◆ **description**

User-defined description.

◆ **glob**

Displays the items that match the `glob` expression. See `help glob` for a description of `glob` expression syntax.

◆ **name**

Specifies the profile instance name. The name must be `classification`. This option is required for the `modify` command.

◆ **partition**

Specifies the administrative partition within which the profile resides.

◆ **regex**

Specifies the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. See `help regex` for a description of regular expression syntax.

◆ **smtp-server**

Specifies the SMTP server configuration to be used with classification for sending reports using email.

See Also

`edit`, `glob`, `list`, `ltm virtual`, `modify`, `regex`, `reset-stats`, `show`, `tmsh`, `sys smtp-server`
client-ssl

Configures a Client SSL profile.

Module

ltm profile

Syntax

Configure the client-ssl component within the ltm profile module using the following syntax.

Create/Modify

create client-ssl [name]
modify client-ssl [name]

options:
  alert-timeout [indefinite | [integer] ]
  allow-non-ssl [disabled | enabled]
  authenticate [always | once]
  authenticate-depth [integer]
  ca-file [name]
  cache-size [integer]
  cache-timeout [integer]
  cert [name]
  chain [name | none]
  ciphers [name | none]
  client-cert-ca [name | none]
  crl-file [name]
  defaults-from [clientssl | [name] ]
  description [string]
  handshake-timeout [indefinite | [integer] ]
  key [ name | none]
  mod-ssl-methods [disabled | enabled]
  mode [disabled | enabled]


  passphrase [ none | [string] ]
  peer-cert-mode [ auto | ignore | request | require]
You can use the `client-ssl` component to create, modify, or delete a custom Client SSL profile, or display a custom or default Client SSL profile. Client-side profiles provide a mechanism for the traffic management system to handle authentication and encryption tasks for any SSL connection coming into a traffic management system from a client system.
Examples

Creates a Client SSL profile named `my_clientssl_profile` using the system defaults:

```plaintext
create clientssl my_clientssl_profile
```

Creates a Client SSL profile named `my_clientssl_profile` using the system defaults, except that a user is authenticated more than once:

```plaintext
create clientssl my_clientssl_profile authenticate-once disabled
```

Options

You can use these options with the `client-ssl` component:

- **alert-timeout**
  Specifies the alert timeout in seconds. The default value is 60 seconds.

- **allow-non-ssl**
  Enables or disables non-SSL connections. Specify `enabled` when you want non-SSL connections to pass through the traffic management system as clear text. The default value is `disabled`.

- **authenticate**
  Specifies how often the system authenticates a user. The default value is `once`.

- **authenticate-depth**
  Specifies the authenticate depth. This is the client certificate chain maximum traversal depth. The default value is 9.

- **ca-file**
  Specifies the certificate authority (CA) file name. Configures certificate verification by specifying a list of client or server CAs that the traffic management system trusts. The default value is `none`.

- **cache-size**
  Specifies the SSL session cache size. For client-side profiles only, you can configure timeout and size values for the SSL session cache. Because each profile maintains a separate SSL session cache, you can configure the values on a per-profile basis. The default value is 20000.

- **cache-timeout**
  Specifies the SSL session cache timeout value. This specifies the number of usable lifetime seconds of negotiated SSL session IDs. The default value is 3600 seconds. Acceptable values are integers greater than or equal to 0 and less than or equal to 86400.

- **cert**
  Specifies the name of the certificate installed on the traffic management system for the purpose of terminating or initiating an SSL connection. You can specify the default certificate name, which is `default.crt`.

- **chain**
  Specifies or builds a certificate chain file that a client can use to authenticate the profile. The default value is `none`. 
- **ciphers**
  Specifies a cipher name. The default value is **DEFAULT**, which uses the default ciphers.

- **client-cert-ca**
  Specifies the client cert certificate authority name. The default value is **none**.

- **crl-file**
  Specifies the certificate revocation list file name. The default value is **none**.

- **defaults-from**
  Specifies the profile that you want to use as the parent profile. Your new profile inherits all settings and values from the parent profile specified. The default value is **clientssl**.

- **description**
  User-defined description.

- **glob**
  Displays the items that match the `glob` expression. For a description of `glob` expression syntax, see the `glob` man page.

- **handshake-timeout**
  Specifies the handshake timeout in seconds. The default value is **60** seconds.

- **key**
  Specifies the name of a key file that you generated and installed on the system. When selecting this option, type a key file name or use the default value **default.key**.

- **mod-ssl-methods**
  Enables or disables ModSSL method emulation. Enable this option when OpenSSL methods are inadequate, for example, when you want to use SSL compression over TLSv1. The default value is **disabled**.

- **mode**
  Specifies the profile mode, which enables or disables SSL processing. The default value is **enabled**.

- **name**
  Specifies a unique name for the component. This option is required for the commands `create`, `delete`, and `modify`.

- **options**
  Enables options, including some industry-related workarounds. Enter options inside braces, for example: **{dont-insert-empty-fragments microsoft-sess-id-bug}**. The default value is **dont-insert-empty-fragments**.

  The options are:
  - **all-bugfixes**
    This option enables the following industry-related defect workarounds: **microsoft-sess-id-bug, netscape-challenge-bug, netscape-reuse-cipher-change-bug, sslref2-reuse-cert-type-bug**.

It is usually safe to use this option to enable the defect workaround options when compatibility with broken implementations is desired. If you edit the configuration in the browser-based Configuration utility, the system expands the all-bugfixes option syntax into each individual option.

- **cipher-server-preference**
  When choosing a cipher, this option uses the server's preferences instead of the client references. When this option is not set, the SSL server always follows the client's references. When this option is set, the SSLv3/TLSv1 server chooses by using its own references. Due to the different protocol, for SSLv2 the server sends its list of preferences to the client, and the client always chooses.

- **dont-insert-empty-fragments**
  Disables a countermeasure against an SSL 3.0/TLS 1.0 protocol vulnerability affecting CBC ciphers. These ciphers cannot be handled by certain broken SSL implementations. This option has no effect for connections using other ciphers.

- **ephemeral-rsa**
  Uses ephemeral (temporary) RSA keys when doing RSA operations. According to the specifications, this is done only when an RSA key can be used for signature operations only (namely under export ciphers with restricted RSA key length). By setting this option, you specify that you want to use ephemeral RSA keys always. This option breaks compatibility with the SSL/TLS specifications and can lead to interoperability problems with clients. Therefore, F5 Networks does not recommend this option. Use ciphers with EDH (ephemeral Diffie-Hellman) key exchange instead. This option is ignored for server-side SSL.

- **microsoft-big-sslv3-buffer**
  Enables a workaround for communicating with older Microsoft® applications that use non-standard SSL record sizes.

- **microsoft-sess-id-bug**
  Handles a Microsoft session ID problem.

- **msie-sslv2-rsa-padding**
  Enables a workaround for communicating with older Microsoft applications that use non-standard RSA key padding. This option is ignored for server-side SSL.

- **netscape-ca-dn-bug**
  Handles a defect regarding the system crashing or hanging. If the system accepts a Netscape Navigator® browser connection, demands a client cert, has a non-self-signed CA that does not have its CA in Netscape, and the browser has a certificate, the system crashes or hangs.

- **netscape-challenge-bug**
  Handles the Netscape challenge problem.
- **netscape-demo-cipher-change-bug**
  Manipulates the SSL server session resumption behavior to mimic that of certain Netscape servers (see the Netscape reuse cipher change bug workaround description). F5 Networks does not recommend this option for normal use. It is ignored for server-side SSL.

- **netscape-reuse-cipher-change-bug**
  Handles a defect within Netscape-Enterprise/2.01, only appearing when connecting through SSLv2/v3 then reconnecting through SSLv3. In this case, the cipher list changes. First, Netscape establishes a connection with the RC4-MD5 cipher list. If the connection is resumed, Netscape switches to using the DES-CBC3-SHA cipher list. However, according to RFC 2246, (section 7.4.1.3, cipher suite) the cipher list is RC4-MD5. As a workaround, you can set Netscape to attempt to connect with a cipher list of DES-CBC-SHA:RC4-MD5, and so on. For some reason, each new connection uses the RC4-MD5 cipher list, but any re-connection attempts to use the DES-CBC-SHA cipher list. Thus Netscape, when reconnecting, always uses the first cipher in the cipher list.

- **no-session-resumption-on-renegotiation**
  When performing renegotiation as an SSL server, this option always starts a new session (that is, session resumption requests are accepted only in the initial handshake). The system ignores this option for server-side SSL.

- **no-sslv2**
  Do not use the SSLv2 protocol.

- **no-sslv3**
  Do not use the SSLv3 protocol.

- **no-tlsv1**
  Do not use the TLSv1 protocol.

- **passive-close**
  Specifies how to handle passive closes.

- **none**
  Disables all workarounds. F5 Networks does not recommend this option.

- **pkcs1-check-1**
  This debugging option deliberately manipulates the PKCS1 padding used by SSL clients in an attempt to detect vulnerability to particular SSL server vulnerabilities. F5 Networks does not recommend this option for normal use. The system ignores this option for client-side SSL.

- **pkcs1-check-2**
  This debugging option deliberately manipulates the PKCS1 padding used by SSL clients in an attempt to detect vulnerability to particular SSL server vulnerabilities. F5 Networks does not recommend this option for normal use. The system ignores this option for client-side SSL.
• **single-dh-use**
  Creates a new key when using temporary/ephemeral DH parameters. This option must be used to prevent small subgroup attacks, when the DH parameters were not generated using strong primes (for example, when using DSA-parameters). If strong primes were used, it is not strictly necessary to generate a new DH key during each handshake, but F5 Networks recommends it. Enable the Single DH Use option whenever temporary or ephemeral DH parameters are used.

• **ssleay-080-client-dh-bug**
  Enables a workaround for communicating with older SSLeay-based applications that specify an incorrect Diffie-Hellman public value length. This option is ignored for server-side SSL.

• **sseref2-reuse-cert-type-bug**
  Handles the SSL reuse certificate type problem.

• **tls-block-padding-bug**
  Enables a workaround for communicating with older TLSv1-enabled applications that use incorrect block padding.

• **tls-d5-bug**
  This option is a workaround for communicating with older TLSv1-enabled applications that specify an incorrect encrypted RSA key length. This option is ignored for server-side SSL.

• **tls-rollback-bug**
  Disables version rollback attack detection. During the client key exchange, the client must send the same information about acceptable SSL/TLS protocol levels as it sends during the first hello. Some clients violate this rule by adapting to the server's answer. For example, the client sends an SSLv2 hello and accepts up to SSLv3.1 (TLSv1), but the server only processes up to SSLv3. In this case, the client must still use the same SSLv3.1 (TLSv1) announcement. Some clients step down to SSLv3 with respect to the server's answer and violate the version rollback protection. The system ignores this option for server-side SSL.

◆ **partition**
  Displays the administrative partition within which the component resides.

◆ **passphrase**
  Specifies the key passphrase, if required. The default value is *none*.

◆ **peer-cert-mode**
  Specifies the peer certificate mode. The default value is *ignore*.

◆ **proxy-ssl**
  Enabling this option requires a corresponding client SSL profile with proxy-ssl enabled to perform transparent SSL decryption. This allows further modification of application traffic within an SSL tunnel while still allowing the server to perform necessary authorization, authentication, and auditing steps.
◆ **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. For a description of regular expression syntax, see the `regex` man page.

◆ **renegotiate-max-record-delay**
  Specifies the maximum number of SSL records that the traffic management system can receive before it renegotiates an SSL session. After the system receives this number of SSL records, it closes the connection. This option applies to client profiles only. The default value is 10.

◆ **renegotiate-period**
  Specifies the number of seconds required to renegotiate an SSL session. The default value is `indefinite`.

◆ **renegotiate-size**
  Specifies the size of the application data, in megabytes, that is transmitted over the secure channel. If the size of the data is higher than this value, the traffic management system must renegotiate the SSL session. The default value is `indefinite`.

◆ **renegotiation**
  Enables or disables renegotiation. The default value is `disabled`.
  If renegotiations are disabled, and the system is acting as an SSL server, and a COMPAT or NATIVE cipher is negotiated, the system aborts the connection. Additionally, when renegotiations are disabled, and the system is acting as an SSL client, the system ignores the server's HelloRequest messages.

◆ **strict-resume**
  Enables or disables strict resume. The default value is `disabled`, which causes the SSL profile to resume an SSL session that was not shut down cleanly. Conversely, you can specify `enabled` to prevent an SSL session from being resumed after an unclean shutdown.

◆ **unclean-shutdown**
  By default, the SSL profile performs unclean shutdows of all SSL connections, which means that underlying TCP connections are closed without exchanging the required SSL shutdown alerts. If you want to force the SSL profile to perform a clean shutdown of all SSL connections, set this option to `disabled`.

---

**See also**

`create`, `delete`, `edit`, `glob`, `list`, `ltm virtual`, `modify`, `regex`, `reset-stats`, `show`, `tmsh`
diameter

Configures a profile to manage Diameter network traffic.

Module

ltm profile

Syntax

Configure the diameter component within the ltm profile module using the following syntax.

Create/Modify

create diameter [name]
modify diameter [name]

options:
  connection-prime [disabled | enabled]
  defaults-from [name]
  description [string]
  destination-realm [string]
  handshake-timeout [number]
  host-ip-rewrite [disabled | enabled]
  max-watchdog-failure [number]
  origin-host [string]
  origin-realm [string]
  overwrite-destination-host [disabled | enabled]
  parent-avp [ [number] | [string] ]
  persist-avp [ [number] | [string] ]
  reset-on-timeout [disabled | enabled]
  watchdog-timeout [number]

edit diameter [ [ [name] | [glob] | [regex] ] ... ]

options:
  all-properties
  non-default-properties
  reset-stats diameter

Display

list diameter
list diameter [ [ [name] | [glob] | [regex] ] ... ]
show running-config diameter
show running-config diameter [ [name] | [glob] | [regex] ] ... ]
  options:
   all-properties
   non-default-properties
   one-line
   partition
  show diameter
show diameter [ [name] | [glob] | [regex] ] ... ]
  options:
   (default | exa | gig | kil | meg | peta | raw | tera | yotta | zetta)
   field-fmt
   global

Delete

delte diameter [name]

Description

You can use the `diameter` component to configure a profile to manage Diameter network traffic.

Examples

Creates a Diameter profile named `my_diameter_profile` that inherits its settings from the system default Diameter profile:

`create diameter my_diameter_profile defaults-from diameter`

Displays the properties of all Diameter profiles:

`list diameter`

Options

You can use these options with the `diameter` component:

- **connection-prime**
  When enabled, and the system receives a capabilities exchange request from the client, the system will establish connections and perform handshaking with all the servers prior to sending the capabilities exchange answer to the client. The default value is `disabled`.

- **defaults-from**
  Specifies the profile that you want to use as the parent profile. Your new profile inherits all settings and values from the parent profile specified. The default value is `diameter`. 
◆ **description**  
User-defined description.

◆ **destination-realm**  
Specifies the realm to which messages are routed. A value of **none** indicates that the *destination-realm* option is **disabled**. The default value is **none**.

You can specify a fully qualified domain name as an ASCII string. For more information about this option, see *RFC 3588 section 6.6*.

◆ **glob**  
Displays the items that match the **glob** expression. For a description of **glob** expression syntax, see the **glob** man page.

◆ **handshake-timeout**  
Specifies the handshake timeout in seconds. This setting specifies the maximum number of seconds that a connection can be idle after the capabilities exchange request was sent to the server. The default value is **10**. The system will reset the connection after it has timed out.

You can specify a numeric value in the range **0** to **4294967295**, the recommended value is in the range of **5** to **30**.

◆ **host-ip-rewrite**  
When **enabled** and the message is a capabilities exchange request or capabilities exchange answer, rewrite the **host-ip-address** attribute with the system’s egress IP address. The default value is **enabled**.

◆ **max-watchdog-failure**  
Specifies the maximum number of device watchdog failures that the traffic management system can take before it tears down the connection. After the system receives this number of device watchdog failures, it closes the connection. The default value is **10**.

You can specify a numeric value in the range **0** to **4294967295**.

◆ **name**  
Specifies the unique name of the component. This option is required.

◆ **overwrite-destination-host**  
When you enable this option, the system replaces the value of the destination host field in the Diameter header with the BIG-IP® pool member address. When you disable this option, the system does not modify the destination host field. The default value is **enabled**.

◆ **parent-avp**  
Specifies the name of the Diameter attribute that the system uses to indicate if the **persist-avp** option is embedded in a grouped avp. A value of **none** indicates that the value of the **persist-avp** option is not embedded in a grouped avp. The default value is **none**.

You can specify an ASCII string or a numeric ID in the range **1** to **4294967295**. Acceptable strings can be found in *RFC 3588 section 4.5*.

◆ **partition**  
Displays the administrative partition within which the component resides.
◆ **persist-avp**
  Specifies the name of the Diameter attribute that the system persists on. A value of none indicates that persistence is disabled. The default value is `session-id`.

You can specify an ASCII string or a numeric ID in the range 1 to `4294967295`. Acceptable strings can be found in RFC 3588 section 4.5.

◆ **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. For a description of regular expression syntax, see the `regex` man page.

◆ **reset-on-timeout**
  When it is `enabled` and the watchdog failures exceed the max watchdog failure, the system resets the connection. The default value is `enabled`.

◆ **watchdog-timeout**
  Specifies the watchdog timeout in seconds. This setting specifies the number of seconds that a connection is idle before the device watchdog request is sent. The default value is 0, which means BIG-IP will not send a device watchdog request to either client or server side.

You can specify a numeric value in the range 0 to `4294967295`, the recommended value is in the range of 6 to 30.

**See also**

create, delete, edit, glob, list, ltm virtual, modify, regex, reset-stats, show, tmsh
**Module**

**ltm profile**

**Syntax**

Configure the dns component within the ltm profile module using the following syntax.

**Create/Modify**

create dns [name]
modify dns [name]

options:
- defaults-from [ [name] | none]
- description [string]
- dns64 [disabled | secondary | immediate | v4-only]
- dns64-additional-section-rewrite [disabled | v6-only | v4-only | any]
- dns64-prefix [IPv6 prefix]
- enable-dnssec [no | yes]
- enable-dns-express [no | yes]
- enable-gtm [no | yes]
- process-rd [no | yes]
- unhandled-query-action [allow | drop | hint | noerror | reject]
- use-local-bind [no | yes]

edit dns [ [ [name] | [glob] | [regex] ] ... ]

options:
- all-properties
- non-default-properties

reset-stats dns

reset-stats dns [ [ [name] | [glob] | [regex] ] ... ]

**Display**

list dns
list dns [ [ [name] | [glob] | [regex] ] ... ]
show running-config dns
show running-config dns [ [ [name] | [glob] | [regex] ] ... ]

options:
Traffic Management Shell (tmsh) Reference Guide

**Delete**

delete dns [name]

**Description**

You can use this component to create, modify, display, or delete a DNS profile to define how the BIG-IP system handles DNS traffic. You can also display and reset DNS profile statistics.

**Examples**

Creates a DNS profile named `my_dns_profile` that inherits its settings from the system default DNS profile:

create dns my_dns_profile defaults-from dns

Displays the properties of all DNS profiles:

list dns

**Options**

You can use these options with the `dns` component:

- **defaults-from**
  Specifies the profile that you want to use as the parent profile. Your new profile inherits all settings and values from the parent profile specified. The default value is `dns`.

- **description**
  User-defined description.

- **dns64**
  Sets DNS64 mapping mode. The default value is `disabled`.

- **dns64-additional-section-rewrite**
  Sets DNS64 additional section rewriting. For AAAA and A records in additional section, this field specifies how they are being rewritten. The default value is `disabled`.

- **dns64-prefix**
  Specifies DNS64 mapping IPv6 prefix.
◆ **enable-dnssec**  
Indicates whether to perform DNS Security Extension (DNSSEC) operations on the DNS packet (for example, respond to DNSKEY queries; add RRSIGs to response).

◆ **enable-dns-express**  
Indicates whether the dns-express service is enabled. The service handles zone transfers from the primary DNS server.

◆ **enable-gtm**  
Indicates whether the Global Traffic Manager™ handles DNS resolution for DNS queries and responses that contain wide IP names. The default value is **yes**.

◆ **glob**  
Displays the items that match the glob expression. For a description of glob expression syntax, see the **glob** man page.

◆ **name**  
Specifies the unique name of the component. This option is required.

◆ **partition**  
Displays the administrative partition within which the component resides.

◆ **process-rd**  
Indicates whether to process clientside DNS packets with Recursion Desired set in the header. The default value is **yes**. If set to **no**, processing of the packet will be subject to the **unhandled-query-action** option.

◆ **regex**  
Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. For a description of regular expression syntax, see the **regex** man page.

◆ **unhandled-query-action**  
Indicates the action to take for a dns query that has not matched any names.

◆ **use-local-bind**  
Indicates whether non-GTM and non-DNS-Express requests should be forwarded to the local BIND.

## See also

`create`, `delete`, `edit`, `glob`, `list`, `ltm virtual`, `modify`, `regex`, `reset-stats`, `show`, `tmsh`
fasthttp

Configures a Fast HTTP profile.

Module

ltm profile

Syntax

Modify the fasthttp component within the ltm profile module using the following syntax.

Create/Modify

create fasthttp [name]
modyify fasthttp [name]

options:
  client-close-timeout [integer]
  connpool-idle-timeout-override [integer]
  connpool-max-reuse [integer]
  connpool-max-size [integer]
  connpool-min-size [integer]
  connpool-replenish [disabled | enabled]
  connpool-step [integer]
  defaults-from [ [name] | none]
  description [string]
  force-http-10-response [disabled | enabled]
  header-insert [none | [string] ]
  http-11-close-workarounds [disabled | enabled]
  idle-timeout [integer]
  insert-xforwarded-for [disabled | enabled]
  layer-7 [disabled | enabled]
  max-header-size [integer]
  max-requests [integer]
  mss-override [integer]
  reset-on-timeout [disabled | enabled]
  server-close-timeout [integer]
  unclean-shutdown [disabled | enabled]

edit fasthttp [ [ [name] | [glob] | [regex] ] ... ]

options:
  all-properties
  non-default-properties
reset-stats fasthttp
reset-stats fasthttp [ [ [name] | [glob] | [regex] ] ... ]
Display

list fasthttp
list fasthttp [ [ [name] | [glob] | [regex] ] ... ]
show running-config fasthttp
show running-config fasthttp [ [ [name] | [glob] | [regex] ] ... ]
  options:
    all-properties
    non-default-properties
    one-line
    partition
show fasthttp
show fasthttp [ [ [name] | [glob] | [regex] ] ... ]
  options:
    (default | exa | gig | kil | meg | peta | raw | tera | yotta | zetta)
    field-fmt
    global

Delete

delete fasthttp [name]

Description

You can use this component to create, modify, display, or delete a Fast HTTP profile. This profile provides the ability to accelerate certain HTTP connections such as banner ads.

Examples

Creates a Fast HTTP profile named my_fast_http_profile that inherits its settings from the system default Fast HTTP profile:

create fasthttp my_fast_http_profile defaults-from fasthttp

Displays fasthttp profile statistics in the system default units:

show fasthttp

Options

You can use the following options with the fasthttp component:

- client-close-timeout
  Specifies the number of seconds after which the system closes a client connection, when the system either receives a client FIN packet or sends a FIN packet. This option overrides the idle-timeout option. The default value is 5.
- **connpool-idle-timeout-override**
  Specifies the number of seconds after which a server connection in a OneConnect™ pool is eligible for deletion, when the connection has no traffic. This option overrides the `idle-timeout` option. The default value is 0 seconds, which disables the override setting.

- **connpool-max-reuse**
  Specifies the maximum number of times that the system can re-use a current connection. The default value is 0 (zero).

- **connpool-max-size**
  Specifies the maximum number of connections to a load balancing pool. A value of 0 (zero) specifies that a pool can accept an unlimited number of connections. The default value is 2048.

- **connpool-min-size**
  Specifies the minimum number of connections to a load balancing pool. The default value of 0 (zero) specifies that there is no minimum.

- **connpool-replenish**
  When enabled, the system replenishes the number of connections to a load balancing pool to the number of connections that existed when the server closed the connection to the pool. The default value is enabled. When disabled, the system replenishes the connection that was closed by the server, only when there are fewer connections to the pool than the number of connections set in the `connpool-min-size` option.

- **connpool-step**
  Specifies the increment at which the system makes additional connections available, when all available connections are in use. The default value is 4.

- **defaults-from**
  Specifies the profile that you want to use as the parent profile. Your new profile inherits all settings and values from the parent profile specified. The default value is fasthttp.

- **description**
  User-defined description.

- **force-http10-response**
  Specifies whether to rewrite the HTTP version in the status line of the server to HTTP 1.0 to discourage the client from pipelining or chunking data. The default value is disabled.

- **glob**
  Displays the items that match the `glob` expression. For a description of `glob` expression syntax, see the `glob` man page.

- **header-insert**
  Specifies a string that the system inserts as a header in an HTTP request. If the header exists already, the system does not replace it. The default value is none.

- **http-11-close-workarounds**
  Enables or disables HTTP 1.1 close workarounds. The default value is disabled.
◆ \textit{idle-timeout}
  Specifies the number of seconds after which a connection is eligible for deletion, when the connection has no traffic. The default value is 300 seconds.

◆ \textit{insert-xforwarded-for}
  Specifies whether the system inserts the \texttt{XForwarded For} header in an HTTP request with the client IP address, to use with connection pooling.
  The options are:
  • \texttt{disabled}
    Specifies that the system does not insert the \texttt{XForwarded For} header.
  • \texttt{enabled}
    Specifies that the system inserts the \texttt{XForwarded For} header with the client IP address.

◆ \textit{layer7}
  When enabled, the system parses HTTP data in the stream. Disable this option if you want to use the performance HTTP profile to shield against denial-of-service attacks against non-HTTP protocols. The default value is \texttt{enabled}.

◆ \textit{max-header-size}
  Specifies the maximum amount of HTTP header data that the system buffers before making a load balancing decision. The default value is 32768.

◆ \textit{max-requests}
  Specifies the maximum number of requests that the system can receive on a client connection, before the system closes the connection. The default value of 0 specifies that requests are not limited.

◆ \textit{mss-override}
  Specifies a maximum segment size (MSS) override for server connections. The default value is 0 (zero), which corresponds to an MSS of 1460. You can specify any integer between 536 and 1460.

◆ \textit{name}
  Specifies a unique name for the component. This option is required for the commands \texttt{create}, \texttt{delete}, and \texttt{modify}.

◆ \textit{partition}
  Displays the administrative partition within which the component resides.

◆ \textit{regex}
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. For a description of regular expression syntax, see the \texttt{regex} man page.

◆ \textit{reset-on-timeout}
  When enabled, the system sends a TCP RESET packet when a connection times out, and deletes the connection. The default value is \texttt{enabled}.

server-close-timeout
Specifies the number of seconds after which the system closes a client connection, when the system either receives a client FIN packet or sends a FIN packet. This option overrides the value of the idle-timeout option. The default value is 5.

unclean-shutdown
Specifies how the system handles closing a connection.
The options are:
- disabled
  Prevents an unclean shutdown of a client connection. This is the default value.
- enabled
  Permits an unclean shutdown of a client connection.
- fast
  Specifies that the system sends a RESET packet to close the connection only if the client attempts to send further data after the response has completed.

See also
create, delete, edit, glob, list, ltm virtual, modify, regex, reset-stats, show, tmsh
fastl4

Configures a Fast Layer 4 profile.

Module

ltm profile

Syntax

Configure the fastl4 component within the ltm profile module using the following syntax.

Create/Modify

create fastl4 [name]
modify fastl4 [name]

options:
  defaults-from [ [name] | none]
  description [string]
  hardware-syn-cookie [disabled | enabled]
  idle-timeout [immediate | indefinite | [integer] ]
  ip-tos-to-client [ [integer] | pass-through]
  ip-tos-to-server [ [integer] | pass-through]
  link-qos-to-client [ [integer] | pass-through]
  link-qos-to-server [ [integer] | pass-through]
  loose-close [disabled | enabled]
  loose-initialization [disabled | enabled]
  mss-override [integer]
  pva-acceleration [full | none | partial]
  reassemble-fragments [disabled | enabled]
  reset-on-timeout [disabled | enabled]
  rtt-from-client [disabled | enabled]
  rtt-from-server [disabled | enabled]
  software-syn-cookie [disabled | enabled]
  tcp-close-timeout [immediate | indefinite | [integer] ]
  tcp-generate-is [disabled | enabled]
  tcp-handshake-timeout [immediate | indefinite | [integer] ]
  tcp-strip-sack [disabled | enabled]
  tcp-timestamp-mode [preserve | rewrite | strip]
  tcp-wscale-mode [preserve | rewrite | strip]
edit fastl4 [ [ [name] | [glob] | [regex] ] ... ]
  options:
    all-properties
    non-default-properties
reset-stats fastl4
  reset-stats fastl4 [ [ [name] | [glob] | [regex] ] ... ]

Display
list fastl4
list fastl4 [ [ [name] | [glob] | [regex] ] ... ]
show running-config fastl4
show running-config fastl4 [ [ [name] | [glob] | [regex] ] ... ]
  options:
    all-properties
    non-default-properties
    one-line
    partition
show fastl4
show fastl4 [ [ [name] | [glob] | [regex] ] ... ]
  options:
    (default | exa | gig | kil | meg | peta | raw | tera | yotta | zetta)
  field-fmt
  global

Delete

delete fastl4 [name]

Description

You can use this component to create, modify, display, or delete a Fast Layer 4 profile. The Fast L4 profile is the default profile that the system uses when you create a basic configuration for non-UDP (User Datagram Protocol) traffic.

Any changes you make to an active Fast L4 profile (one that is in use by a virtual server) take effect after the value of the idle-timeout option has passed. That means new connections are affected by the profile change immediately. However, for the new values to take effect, old connections need to be either aged out or closed.
Examples

Creates a custom Fast Layer 4 profile named `my_fastl4_profile` that inherits its settings from the system default `fastl4` profile:

```
create fastl4 my_fastl4_profile defaults-from fastl4
```

Displays statistics for all Fast Layer 4 profiles:

```
show fastl4
```

Options

You can use these options with the `fastl4` component:

- **defaults-from**
  Specifies the profile that you want to use as the parent profile. Your new profile inherits all settings and values from the parent profile specified. The default value is `fastl4`.

- **description**
  User-defined description.

- **glob**
  Displays the items that match the `glob` expression. For a description of `glob` expression syntax, see the `glob` man page.

- **hardware-syn-cookie**
  Enables or disables hardware SYN cookie support when PVA10 is present on the system. The default value is `disabled`.
  When you set the `hardware-syn-cookie` option to `enabled`, you can also want to set the following `bigdb` database variables using the `db` component, based on your requirements:
  - `pva.SynCookies.ClientWindow` (default: 0)

- **idle-timeout**
  Specifies the number of seconds that a connection is idle before the connection is eligible for deletion. The default value is 300 seconds. You can also specify `immediate` or `indefinite`.
  When you specify an idle timeout for the Fast L4 profile, for the profile to work properly, the value needs to be greater than the bigdb database variable `Pva.Scrub_time_in_msec`.

- **ip-tos-to-client**
  Specifies an IP Type of Service (ToS) number for the client side. This option specifies the ToS level that the traffic management system assigns to UDP packets when sending them to clients. The default value is `65535`, which indicates, do not modify UDP packets.
◆ ip-tos-to-server
Specifies an IP ToS number for the server side. This option specifies the ToS level that the traffic management system assigns to UDP packets when sending them to servers. The default value is 65535, which indicates, do not modify UDP packets.

◆ link-qos-to-client
Specifies the Link Quality of Service (QoS) (VLAN priority) number for the client side. This option specifies the QoS level that the system assigns to UDP packets when sending them to clients. The default value is 65535, which indicates, do not modify UDP packets.

◆ link-qos-to-server
Specifies a Link QoS (VLAN priority) number for the server side. This option specifies the QoS level that the system assigns to UDP packets when sending them to servers. The default value is 65535, which indicates, do not modify UDP packets.

◆ loose-close
Specifies that the system closes a loosely initiated connection when the system receives the first FIN packet from either the client or the server. The default value is disabled.

◆ loose-initialization
Specifies that the system initializes a connection when it receives any Transmission Control Protocol (TCP) packet, rather than requiring a SYN packet for connection initiation. The default value is disabled.

◆ mss-override
Specifies a maximum segment size (MSS) override for server connections. Note that this is also the MSS advertised to a client when a client first connects.

The default value is 0 (zero), which disables this option. You can specify an integer from 256 to 9162.

◆ name
Specifies a unique name for the component. This option is required for the commands create, delete, and modify.

◆ partition
Displays the administrative partition within which the component resides.

◆ pva-acceleration
Specifies the Packet Velocity® ASIC acceleration mode. The default value is full.

◆ reassemble-fragments
Specifies whether to reassemble fragments. The default value is disabled.

◆ regex
Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. For a description of regular expression syntax, see the regex man page.
reset-on-timeout
Specifies whether you want to reset connections on timeout. The default value is enabled.

rtt-from-client
Enables or disables the TCP timestamp options to measure the round trip time to the client. The default value is disabled.

rtt-from-server
Enables or disables the TCP timestamp options to measure the round trip time to the server. The default value is disabled.

software-syn-cookie
Enables or disables software SYN cookie support when PVA10 is not present on the system. The default value is disabled.

tcp-close-timeout
Specifies a TCP close timeout in seconds. You can also specify immediate or indefinite. The default value is 5 seconds.

tcp-generate-isn
Specifies whether you want to generate TCP sequence numbers on all synchronizations that conform with RFC1948, and allow timestamp recycling. The default value is disabled.

tcp-handshake-timeout
Specifies a TCP handshake timeout in seconds. You can also specify immediate or indefinite. The default value is 5 seconds.

tcp-strip-sack
Specifies whether you want to block the TCP SackOK option from passing to the server on an initiating SYN. The default value is disabled.

tcp-timestamp-mode
Specifies how you want to handle the TCP timestamp. The default value is preserve.

tcp-wscale-mode
Specifies how you want to handle the TCP window scale. The default value is preserve.

See also
create, delete, edit, glob, list, ltm virtual, modify, regex, reset-stats, show, tmsh
ftp

Configures an FTP profile.

Module

ltm profile

Syntax

Configure the ftp component within the ltm profile module using the following syntax.

Create/Modify

create ftp [name]
modify ftp [name]
  options:
    defaults-from [ [name] | none]
    description [string]
    port [name]
    security [disabled | enabled]
    translate-extended [disabled | enabled]
edit ftp [ [ [name] | [glob] | [regex] ] ... ]
  options:
    all-properties
    non-default-properties

Display

list ftp
list ftp [ [ [name] | [glob] | [regex] ] ... ]
show running-config ftp
show running-config ftp [ [ [name] | [glob] | [regex] ] ... ]
  options:
    all-properties
    non-default-properties
    one-line
    partition

Delete

delete ftp [name]
Description

You can use the ftp component to create, modify, display, or delete an FTP profile with which you can manage FTP traffic.

Examples

Creates a custom FTP profile named my_ftp_profile that inherits its settings from the system default FTP profile:

```
create ftp my_ftp_profile defaults-from ftp
```

Displays the properties of all FTP profiles:

```
list ftp
```

Options

You can use these options with the ftp component:

- **defaults-from**
  Specifies the profile that you want to use as the parent profile. Your new profile inherits all settings and values from the parent profile specified. The default value is ftp.

- **description**
  User-defined description.

- **glob**
  Displays the items that match the glob expression. For a description of glob expression syntax, see the glob man page.

- **name**
  Specifies a unique name for the component. This option is required for the commands create, delete, and modify.

- **partition**
  Displays the administrative partition within which the component resides.

- **port**
  Specifies a service for the data channel port used for this FTP profile. The default value is ftp-data.

- **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. For a description of regular expression syntax, see the regex man page.

- **security**
  Enables or disables secure FTP traffic for the BIG-IP Application Security Manager™. You can set the security option only if the system is licensed for the BIG-IP Application Security Manager. The default value is disabled.
translate-extended
This option is enabled by default, and thus, automatically translates RFC2428 extended requests EPSV and EPRT to PASV and PORT when communicating with IPv4 servers.

See also

create, delete, edit, glob, list, ltm virtual, modify, regex, reset-stats, show, tmsh
http

Configures an HTTP profile.

Module

ltm profile

Syntax

Configure the http component within the ltm profile module using the following syntax.

Create/Modify

create http [name]
modify http [name]

options:
   basic-auth-realm [ "string" ] | none
   defaults-from [ [name] | none]
   description [string]
   encrypt-cookie-secret [none | [passphrase] ]
   encrypt-cookies
      [add | delete | replace-all-with] {
          [cookie] ...
      }
   encrypt-cookies none
   fallback-host [ [hostname] | none]
   fallback-status-codes
      [add | delete | replace-all-with] {
          [fallback status code]...
      }
   fallback-status-codes none
   header-erase [none | [string] ]
   header-insert [none | [string] ]
   insert-xforwarded-for [disabled | enabled]
   lws-separator
   lws-width [integer]
   max-header-size [integer]
   max-header-count [integer]
   max-requests [integer]
   oneconnect-transformations [disabled | enabled]
   pipelining [disabled | enabled]
   redirect-rewrite [all | matching | nodes | none]
request-chunking [preserve | rechunk | selective | unchunk]
response-chunking [preserve | rechunk | selective | unchunk]
response-headers-permitted
  [add | delete | replace-all-with] {
    [response header] ...
  }
response-headers-permitted none
via-host-name [string]
via-request [append | preserve | remove]
via-response [append | preserve | remove]
security [disabled | enabled]
edit http [ [name] | [glob] | [regex] ] ...
  options:
    all-properties
    non-default-properties
reset-stats http
reset-stats http [ [name] | [glob] | [regex] ] ...

Display
list http
list http [ [name] | [glob] | [regex] ] ...
show running-config http
show running-config http [ [name] | [glob] | [regex] ] ...
  options:
    all-properties
    non-default-properties
    one-line
    partition
show http
show http [ [name] | [glob] | [regex] ] ...
  options:
    (default | exa | gig | kil | meg | peta | raw | tera | yotta | zetta)
    field-fmt
    global

Delete
  delete http [name]
Description

You can use the `http` component to create, modify, display, or delete an HTTP profile.

The BIG-IP system installation includes the following default HTTP-type profile: `http`. The default HTTP profile contains values for properties related to managing HTTP traffic.

You can create a new HTTP-type profile using an existing profile as a parent profile, and then you can change the values of the properties to suit your needs.

Examples

Creates a custom HTTP profile named `my_http_profile` that inherits its settings from the system default HTTP profile:

```
create http my_http_profile defaults-from http
```

Options

You can use these options with the `http` component:

- **basic-auth-realm**
  Specifies a quoted string for the basic authentication realm. The system sends this string to a client whenever authorization fails. The default value is `none`.

- **defaults-from**
  Specifies the profile that you want to use as the parent profile. Your new profile inherits all settings and values from the parent profile specified. The default value is `none`.

- **description**
  User-defined description.

- **encrypt-cookie-secret**
  Specifies a passphrase for the cookie encryption. The default value is `none`.

- **encrypt-cookies**
  Encrypts specific cookies that the BIG-IP system sends to a client system. The default value is `none`.

- **fallback-host**
  Specifies an HTTP fallback host. The default value is `none`.
  With HTTP redirection, you can redirect HTTP traffic to another protocol identifier, host name, port number, or URI path. For example, if all members of a targeted pool are unavailable (that is, the members are disabled, marked as `down`, or have exceeded their connection limit), the system can redirect the HTTP request to the fallback host, with the HTTP reply `Status Code 302 Found`.

- **fallback-status-codes**
  Specifies one or more three-digit status codes that can be returned by an HTTP server. The default value is `none`. 
◆ **glob**
  Displays the items that match the glob expression. For a description of glob expression syntax, see the glob man page.

◆ **header-erase**
  Specifies the header string that you want to erase from an HTTP request. The default value is none.

◆ **header-insert**
  Specifies a quoted header string that you want to insert into an HTTP request. The default value is none.
  The HTTP header being inserted can include a client IP address. Including a client IP address in an HTTP header is useful when a connection goes through a secure network address translation (SNAT) and you need to preserve the original client IP address. When you assign the configured HTTP profile to a virtual server, the system then inserts the header specified by the profile into any HTTP request that the system sends to a pool or pool member.

◆ **insert-xforwarded-for**
  Enables or disables insertion of an X-Forwarded-For header. The default value is disabled.
  When using connection pooling, which allows clients to make use of other client requests' server connections, you can insert the X-Forwarded-For header and specify a client IP address.

◆ **lws-separator**
  Specifies the linear white space separator that the system uses between HTTP headers when a header exceeds the maximum width specified in the lws-width option. The default value is none.

◆ **lws-width**
  Specifies the maximum number of columns that a header that is inserted into an HTTP request can have. See also the lws-separator option, preceding. The default value is 80.

◆ **max-header-size**
  Specifies the maximum header size. The default value is 32768.

◆ **max-header-count**
  Specifies the maximum number of headers in HTTP request or response that will be handled. If client or server sends request or response with the number of headers greater then specified, the connection will be dropped. The default value is 64.

◆ **max-requests**
  Specifies the number of requests that the system accepts on a per-connection basis. The default value is 0 (zero), which means the system does not limit the number of requests per connection.

◆ **name**
  Specifies a unique name for the component. This option is required for the commands create, delete, and modify.
◆ **oneconnect-transformations**
   Specifies whether the system performs HTTP header transformations for the purpose of keeping server connections open. The default value is enabled. This feature requires configuration of a OneConnect profile.

◆ **partition**
   Displays the administrative partition within which the component resides.

◆ **pipelining**
   Enables or disables HTTP/1.1 pipelining. The default value is enabled, which means that clients can make requests even when prior requests have not received a response. For this to succeed, however, destination servers must include support for pipelining.

◆ **redirect-rewrite**
   Specifies which of the application HTTP redirects the system rewrites to HTTPS.
   The options are:
   * all
     Rewrites all application redirects to HTTPS.
   * matching
     Rewrites only application redirects that match the original URI exactly to HTTPS.
   * nodes
     If the URI contains a node IP address, instead of a host name, specifies that the system rewrites the node IP address to the virtual server IP address.
   * none
     Specifies that the system does not rewrite application HTTP redirects to HTTPS. This is the default value.

   Use this feature when an application is generating HTTP redirects that send the client to HTTP (a non-secure channel) when you want the client to continue accessing the application using HTTPS (a secure channel). This is a common occurrence when using client SSL processing on a BIG-IP system.

◆ **regex**
   Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. For a description of regular expression syntax, see the regex man page.

◆ **response-chunking**
   Specifies how to handle chunked and unchunked requests and responses. The default value is selective.
   The options are:
   * unchunk
     If the request or response is chunked, this option unchunks the request or response, processes the HTTP content, and passes on the request or response as unchunked. The Keep-Alive value for the Connection header is not supported, and therefore the system sets the value of the
header to Close. If the request or response is unchunked, the BIG-IP Local Traffic Manager system processes the HTTP content and passes the request or response on untouched.

- **rechunk**
  If the request or response is chunked, the system unchunks the request or response, processes the HTTP content, re-adds the chunk trailer headers, and then passes on the request or response as chunked. Any chunk extensions are lost. If the request or response is unchunked, the system adds transfer encoding and chunking headers on egress.

- **preserve**
  Specifies that the system processes the HTTP content, and sends the response to the client unchanged.

- **selective**
  If the request or response is chunked, the system unchunks the request or response, processes the HTTP content, re-adds the chunk trailer headers, and then passes on the request or response as chunked. Any chunk extensions are lost. If the request is unchunked, the system processes the HTTP content, and then passes on the request or response untouched.

- **response-headers-permitted**
  Specifies the headers that the BIG-IP system accepts in an HTTP response. The default value is `none`.

- **via-host-name**
  Specifies the hostname that will be used in the `Via: HTTP` header. See `via-request` and `via-response` for how the `Via: header` will be handled. If either `via-request` or `via-response` are set to `append`, then this is required.

- **via-request**
  Specifies how you want to process `Via: HTTP` header in requests sent to OWS. The default setting is `remove`. The available values are:
  - **append**
    The value from `via-host-name` is appended to the `Via: HTTP` header.
  - **preserve**
    `Via: HTTP` header is preserved without changes.
  - **remove**
    `Via: HTTP` header is removed from the request.

- **via-response**
  Specifies how you want to process `Via: HTTP` header in responses sent to clients. The default setting is `remove`. The available values are the same as in `via-request`.

- **security**
  Specifies whether the system uses Halon Scripting Language (HSL) security checking. The default value is `disabled`.

### See also

`create`, `delete`, `edit`, `glob`, `list`, `ltm profile fasthttp`, `ltm virtual`, `modify`, `regex`, `reset-stats`, `show`, `tmsh`
httpclass

Configures an HTTP Class type of profile.

Module

ltm profile

Syntax

Configure the httpclass component within the ltm profile module using the following syntax.

Create/Modify

create httpclass [name]
modify httpclass [name]
options:
  asm [disabled | enabled]
  cookies [add | delete | replace-all-with] \n    { [regex:[cookie] ... ] | [glob:[cookie] ... ] }
  cookies none
  defaults-from [ [name] | none]
  description [string]
  headers [add | delete | replace-all-with] \n    { [regex:[header] ... ] | [glob:[header] ... ] }
  headers none
  hosts [add | delete | replace-all-with] \n    { [regex:[host] ... ] | [glob:[host] ... ] }
  hosts none
  paths [add | delete | replace-all-with] \n    { [regex:[path] ... ] | [glob:[path] ... ] }
  paths none
  pool [ [name] | none]
  redirect [none | [URL] ]
  url-rewrite [none | [Tcl expression] ]
  web-accelerator [disabled | enabled]
edit httpclass [ [ [name] | [glob] | [regex] ] ... ]
options:
  all-properties
  non-default-properties
reset-stats httpclass
reset-stats httpclass [ [ [name] | [glob] | [regex] ] ... ]
Display

list httpclass
list httpclass [ [ [name] | [glob] | [regex] ] ... ]
show running-config httpclass
show running-config httpclass [ [ [name] | [glob] | [regex] ] ... ]
    options:
        all-properties
        non-default-properties
        one-line
        partition
show httpclass
show httpclass [ [ [name] | [glob] | [regex] ] ... ]
    options:
        (default | exa | gig | kil | meg | peta | raw | tera | yotta | zetta)
        field-fmt
        global

Delete

delete httpclass [name]

Description

You can use the httpclass component to create an HTTP class profile, redirect HTTP traffic to HTTPS using the same virtual server, and redirect HTTP traffic without changing the URL in the browser.

Examples

Creates an HTTP class profile named my_httpclass_profile that inherits its settings from the system default HTTP Class profile:
create httpclass my_httpclass_profile defaults-from httpclass

Displays all properties for all HTTP Class profiles:
list httpclass all-properties

Options

You can use the following options with the httpclass component:

- **asm**
  Enables or disables application security management. You can set the asm option only if the system is licensed for the BIG-IP Application Security Manager. The default value is **disabled**.
cookies
Specifies how the system routes all incoming HTTP traffic for the web application, based on cookie headers. The value requires a prefix of either regex: or glob:, for example: regex:cookie1, regex:cookie2, or glob:cookie3. The default value is none.

defaults-from
Specifies the profile that you want to use as the parent profile. Your new profile inherits all settings and values from the parent profile specified. The default value is httpclass.
description
User-defined description.
glob
Displays the items that match the glob expression. For a description of glob expression syntax, see the glob man page.
headers
Specifies how the system routes incoming HTTP traffic for the web application, based on HTTP headers and values. The value requires a prefix of either regex: or glob:, for example: regex:header1, regex:header2, or glob:header3. The default value is none.
hosts
Specifies how the system routes incoming HTTP traffic, based on host information. The value requires a prefix of either regex: or glob:, for example: regex:host1, regex:host2, or glob:host3. The default value is none.
name
Specifies a unique name for the component. This option is required for the commands create, delete, and modify.
partition
Displays the administrative partition within which the component resides.
paths
Specifies how the system routes all incoming HTTP traffic for the web application, based on URI paths. The value requires a prefix of either regex: or glob:, for example: regex:path1, regex:path2, glob:path3. The default value is none.

pool
Specifies a local traffic pool to which the system sends the HTTP traffic. The default value is none.
redirect
Specifies a URL to which the system redirects the traffic. The default value is none.
regex
Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. For a description of regular expression syntax, see the regex man page.
- **url-rewrite**
  Specifies the Tcl expression that the system uses to rewrite the request URI that is forwarded to the server without sending an HTTP redirect to the client. The default value is **none**.

- **web-accelerator**
  Specifies web acceleration. You can set this option only if the system is licensed for the BIG-IP WebAccelerator™ system. The default value is **disabled**.

**See also**

create, delete, edit, glob, list, ltm profile fasthttp, ltm profile http, ltm virtual, modify, regex, reset-stats, show, tmsh
http-compression

Configures an HTTP Compression profile.

Module

ltm profile

Syntax

Configure the http-compression component within the ltm profile module using the following syntax.

Create/Modify

create http-compression [name]
modify http-compression [name]

options:
  allow-http-10 [disabled | enabled]
  browser-workarounds [disabled | enabled]
  buffer-size [integer]
  cpu-saver [disabled | enabled]
  cpu-saver-high [integer]
  cpu-saver-low [integer]
  content-type-exclude
    [add | delete | replace-all-with] {
      [content type] ... 
    }
  content-type-exclude none
  content-type-include
    [add | delete | replace-all-with] {
      [content type] ... 
    }
  content-type-include none
  defaults-from [ [name] | none]
  description [string]
  gzip-level [integer]
  gzip-memory-level [integer, in bytes]
  gzip-window-size [integer]
  keep-accept-encoding [disabled | enabled]
  method-prefer [deflate | gzip]
  min-size [integer]
  selective [disabled | enabled]
  uri-exclude
[add | delete | replace-all-with] {
    [URI] ...
}
uri-exclude none
uri-include
    [add | delete | replace-all-with] {
        [URI] ...
    }
uri-include none
vary-header [disabled | enabled]
edit http-compression [ [ [name] | [glob] | [regex] ] ... ]
options:
    all-properties
    non-default-properties
reset-stats http-compression
reset-stats http-compression [ [ [name] | [glob] | [regex] ] ... ]

Display
list http-compression
list http-compression [ [ [name] | [glob] | [regex] ] ... ]
show running-config http-compression
show running-config http-compression [ [ [name] | [glob] | [regex] ] ... ]
options:
    all-properties
    non-default-properties
    one-line
    partition
show http-compression
show http-compression [ [ [name] | [glob] | [regex] ] ... ]
options:
    (default | exa | gig | kil | meg | peta | raw | tera | yotta | zetta)
    field-fmt
global

Delete
    delete http-compression [name]

Description
You can use the http-compression component to create, modify, display, or delete an HTTP Compression profile.
The BIG-IP system installation includes the following default HTTP Compression-type profiles:

- http-compression
- wan-optimized-compression

The default HTTP Compression profile contains values for properties related to managing compression settings.

You can create a new HTTP Compression-type profile using an existing profile as a parent profile, and then you can change the values of the properties to suit your needs.

**Examples**

Creates a custom HTTP Compression profile named `my_hc_profile` that inherits its settings from the system default HTTP Compression profile:

```
create http-compression my_hc_profile defaults-from http-compression
```

**Options**

You can use these options with the `ftp` component:

- **allow-http10**
  Enables or disables compression of HTTP/1.0 server responses. The default value is `disabled`.

- **browser-workarounds**
  Enables or disables compression of browser workarounds. The default value is `disabled`. Enabling this options turns off compression on server responses when any of the following conditions are detected:
  
  - If the client browser is Netscape Navigator® version 4.0x, compression is turned off. Netscape advertises that the browser can handle compression gracefully. In this case, F5 Networks disables compression entirely for that class of browser.
  
  - If the client browser is Netscape Navigator version 4.x (4.10 and beyond) and the server response Content-Type is not either text/html or text/plain compression is turned off. This class of Netscape browsers can handle plain text and HTML just fine, but there are known issues with other types of content.
  
  - If the client browser is Microsoft® Internet Explorer (any version), the server response Content-Type is either text/css or application/x-javascript, and the server sets the header Cache-Control to no-cache, compression is turned off. The Microsoft article ID for this problem is 825057.
  
  - If the client browser is Microsoft Internet Explorer (any version), the server response Content-Type is either text/css or application/x-javascript, and the server sets the header Cache-Control to no-cache, compression is turned off. The Microsoft article ID for this problem is 327286.
• **buffer-size**
  Specifies the maximum number of uncompressed bytes that the system buffers before determining whether to compress the response. Useful when the headers of a server response do not specify the length of the response content. The default value is 4096.

• **content-type-exclude**
  Specifies a string list of HTTP Content-Type responses that you do not want the system to compress. The default value is none.

• **content-type-include**
  Specifies a string list of HTTP Content-Type responses that you want the system to compress. The default value is \{ text/application/(xml|x-javascript) \}.

• **cpu-saver**
  Enables or disables the CPU saver feature. When the CPU saver is enabled, the system monitors the percent of CPU usage and adjusts compression rates automatically when the CPU usage reaches the percentage defined in the `compress-cpu-saver-low` and `compress-cpu-saver-high` options. The default value is enabled.

• **cpu-saver-high**
  Specifies the percent of CPU usage at which the system starts automatically decreasing the amount of content being compressed, as well as the amount of compression that the system is applying. The default value is 90.

• **cpu-saver-low**
  Specifies the percent of CPU usage at which the system resumes content compression at the user-defined rates. The default value is 75.

• **defaults-from**
  Specifies the profile that you want to use as the parent profile. Your new profile inherits all settings and values from the parent profile specified. The default value is none.

• **description**
  User defined description.

• **gzip-level**
  Specifies a value that determines the amount of memory that the system uses when compressing a server response. The default value is 1.

• **gzip-memory-level**
  Specifies the amount of memory (in kilobytes) that the system uses when compressing a server response. The system rounds the value up to the nearest power of two. The default value is 8. The maximum value is 256.

• **gzip-window-size**
  Specifies the number of kilobytes in the window size that the system uses when compressing a server response. The system rounds the value up to the nearest power of two. The default value is 16. The maximum value is 128.

• **keep-accept-encoding**
  Specifies where data compression is performed. When enabled, the target server, rather than the BIG-IP Local Traffic Manager system, performs data compression. The default value is disabled.
◆ **method-prefer**
   Specifies the type of compression that the system prefers. The default value is `gzip`.

◆ **min-size**
   Specifies the minimum length in bytes of a server response that is acceptable for compression. The length in bytes applies to content length only, not headers. The default value is `1024`.

◆ **partition**
   Displays the administrative partition within which the profile resides.

◆ **selective**
   Enables or disables selective compression mode. Note that the data compression feature compresses HTTP server responses, and not client requests. The default value is `disabled`.

◆ **uri-exclude**
   Disables compression on a specified list of HTTP Request-URI responses. Use a regular expression to specify a list of URIs you do not want to compress. The default value is `none`.

◆ **uri-include**
   Enables compression on a specified list of HTTP Request-URI responses. Use a regular expression to specify a list of URIs you want to compress. The default value is `none`.

◆ **vary-header**
   Enables or disables the insertion of a Vary header into cacheable server responses. The default value is `enabled`.

---

**See also**

create, delete, edit, glob, list, ltm virtual, modify, regex, reset-stats, show, tmsh
**iiop**

Configures an Internet Inter-Orb Protocol (IIOP) profile.

**Module**

**ltm profile**

**Syntax**

Configure the **iiop** component within the **ltm profile** module using the following syntax.

**Create/Modify**

```plaintext
create iiop [name]
modify iiop [name]
  options:
    abort-on-timeout [disabled | enabled]
    defaults-from [name]
    description [string]
    partition
    persist-object-key [disabled | enabled]
    persist-request-id [disabled | enabled]
    timeout [integer]
edit iiop [ [ [name] | [glob] | [regex] ] ... ]
  options:
    all-properties
    non-default-properties
reset-stats iiop
reset-stats [ [ [name] | [glob] | [regex] ] ... ]
```

**Display**

```plaintext
list iiop
list iiop [ [ [name] | [glob] | [regex] ] ... ]
show running-config iiop
show running-config iiop [ [ [name] | [glob] | [regex] ] ... ]
  options:
    all-properties
    non-default-properties
    one-line
    partition
```
show iiop
show iiop [ [ [name] | [glob] | [regex] ] ... ]

options:
   (default | exa | gig | kil | meg | peta | raw | tera | yotta | zetta)
   field-fmt
global

Delete

delete iiop [name]

Description

You can use the iiop component to manage IIOP network traffic. The system parses the incoming TCP stream, disaggregates it into IIOP messages, and performs load balancing and persistence based on the parameters you set.

Examples

Creates an IIOP profile named my_iiop_profile that inherits its settings from the system default IIOP profile:
create iiop my_iiop_profile defaults-from iiop

Displays all properties for all IIOP profiles:
list iiop all-properties

Options

You can use the following options with the iiop component:

- **abort-on-timeout**
  Specifies whether the system aborts the connection if there is no response received within the time specified in the timeout option. The default value is disabled.

- **defaults-from**
  Specifies the profile that you want to use as the parent profile. Your new profile inherits all settings and values from the parent profile specified. The default value is iiop.

- **description**
  User-defined description.

- **glob**
  Displays the items that match the glob expression. For a description of glob expression syntax, see the glob man page.

- **name**
  Specifies a unique name for the component. This option is required for the commands create, delete, and modify.
◆ partition
Displays the administrative partition within which the component resides.

◆ persist-object-key
Specifies whether to persist connections based on the object key in the IIOP request. The default value is disabled.

◆ persist-request-id
Specifies whether to persist connections based on the request ID in the IIOP request. The default value is enabled.

◆ regex
Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. For a description of regular expression syntax, see the regex man page.

◆ timeout
Specifies the request timeout. The system uses this value when the abort-on-timeout option is enabled. The default value is 30 seconds.

See also

create, delete, edit, glob, list, ltm virtual, modify, regex, reset-stats, show, tmsh
mblb

Configures an MBLB profile (experimental).

Module

ltm profile

Syntax

Configure the mblb component within the ltm profile module using the syntax shown in the following sections.

Create/Modify

create mblb [name]
modify mblb [name]
  options:
    defaults-from [ [name] | none]
    description [string]
    isolate-abort [disabled | enabled]
    isolate-expire [disabled | enabled]
    isolate-server [disabled | enabled]
    isolate-client [disabled | enabled]
    ingress-high [# of messages]
    ingress-low [# of messages]
    min-conn [# of connections]
edit mblb [ [ [name] | [glob] | [regex] ] ... ]
  options:
    all-properties
    non-default-properties

Display

list mblb
list mblb [ [ [name] | [glob] | [regex] ] ... ]
show running-config mblb
show running-config mblb [ [ [name] | [glob] | [regex] ] ... ]
  options:
    all-properties
    non-default-properties

Delete

delete mblb [name]
Description

Use this command to create, modify, display, or delete an MBLB profile with which you can customize MBLB behavior.

Examples

Creates a custom MBLB profile named `my_mblb_profile` that inherits its settings from the system default MBLB profile:

```
create mblb my_mblb_profile defaults-from mblb
```

Displays the properties of all MBLB profiles:

```
list mblb
```

Options

You can use these options with the `mblb` component:

- **defaults-from**
  Specifies the profile that you want to use as the parent profile. Your new profile inherits all settings and values from the parent profile specified. The default value is `mblb`.

- **description**
  User-defined description.

- **glob**
  Displays the items that match the `glob` expression. See `help glob` for a description of `glob` expression syntax.

- **name**
  Specifies a unique name for the component. This option is required for the commands `create`, `delete`, and `modify`.

- **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. See `help regex` for a description of regular expression syntax.

- **isolate-abort**
  Specify whether to isolate abort event propagation.

- **isolate-expire**
  Specify whether to isolate expiration event propagation.

- **isolate-server**
  Specify whether to isolate serverside shutdown event propagation. This also dominate serverside abort/expiration event propagation.

- **isolate-client**
  Specify whether to isolate clientside shutdown event propagation. This also dominate clientside abort/expiration event propagation.
◆ ingress-high
Specify the high water mark for ingress message queue

◆ ingress-low
Specify the low water mark for ingress message queue

◆ min-conn
Specify the minimum number of serverside connections

See also

create, delete, edit, glob, list, ltm virtual, modify, regex, reset-stats, show, sys provision, tmsh
ntlm

Configures a Microsoft Windows® NT Local Area Network (LAN) manager profile.

Module

ltm profile

Syntax

Configure the ntlm component within the ltm profile module using the following syntax.

Create/Modify

create ntlm [name]
modify ntlm [name]
   options:
     defaults-from [name]
     description [string
     insert-cookie-domain
     insert-cookie-name [cookie name]
     insert-cookie-passphrase [passphrase]
     key-by-cookie [disabled | enabled]
     key-by-cookie-name [cookie name]
     key-by-domain [disabled| enabled]
     key-by-ip-address [disabled | enabled]
     key-by-target [disabled| enabled]
     key-by-user [disabled | enabled]
     key-by-workstation [disabled| enabled]
edit ntlm [ [ [name] | [glob] | [regex] ] ... ]
   options:
     all-properties
     non-default-properties

Display

list ntlm
list ntlm [ [ [name] | [glob] | [regex] ] ... ]
show running-config ntlm
show running-config ntlm [ [ [name] | [glob] | [regex] ] ... ]
   options:
     all-properties
Delete

delete ntlm [name]

Description

You can use the ntlm component to create a Microsoft Windows NT LAN manager (NTLM) profile to manage servers on the LAN that are running Windows NT.

Examples

Creates a Microsoft Windows NT LAN manager profile named my_ntlm_profile that inherits its settings from the system default NTLM profile named ntlm:

create ntlm my_ntlm_profile defaults-from ntlm

Displays all properties for all NTLM profiles:

list ntlm all-properties

Options

You can use these options with the ntlm component:

- defaults-from
  Specifies the profile that you want to use as the parent profile. Your new profile inherits all settings and values from the parent profile specified. The default value is ntlm.

- description
  User-defined description.

- glob
  Displays the items that match the glob expression. For a description of glob syntax, see the glob man page.

- insert-cookie-domain
  Specifies an optional domain for the inserted cookie. The default value is none, which causes no domain to be configured for the inserted cookie.

- insert-cookie-name
  Specifies a cookie name that the system inserts in the cookie. The default value is NTLMconnpool.

- insert-cookie-passphrase
  Specifies a cookie passphrase that the system inserts in the cookie. The default value is mypassphrase.
◆ **key-by-cookie**
   Specifies whether the system uses the existing cookie as the key. The default value is disabled.

◆ **key-by-cookie-name**
   Specifies whether the system uses the value of the insert-cookie-name option as the key. The default value is mycookie.

◆ **key-by-domain**
   Specifies whether the system uses the NTLM domain as the key. The default value is disabled.

◆ **key-by-ip-address**
   Specifies whether the system uses the client IP address as the key. The default value is disabled.

◆ **key-by-target**
   Specifies whether the system uses the NTLM target as the key. The default value is disabled.

◆ **key-by-user**
   Specifies whether the system uses the NTLM user as the key. The default value is enabled.

◆ **key-by-workstation**
   Specifies whether the system uses the NTLM workstation as the key. The default value is disabled.

◆ **name**
   Specifies a unique name for the component. This option is required for the commands create, delete, and modify.

◆ **regex**
   Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. For a description of regular expression syntax, see the regex man page.

---

**See also**

create, delete, edit, glob, list, ltm profile auth, ltm virtual, modify, regex, show, tmsh
one-connect

Configures a OneConnect profile.

Module

ltm profile

Syntax

Configure the one-connect component within the ltm profile module using the following syntax.

Create/Modify

create one-connect [name]
modify one-connect [name]
  options:
    defaults-from [name]
    description [string]
    idle-timeout-override [disabled | enabled]
    max-age [integer]
    max-reuse [integer]
    max-size [integer]
    source-mask [ip address]
edit one-connect [ [ [name] | [glob] | [regex] ] ... ]
  options:
    all-properties
    non-default-properties
reset-stats one-connect
reset-stats one-connect [ [ [name] | [glob] | [regex] ] ... ]

Display

list one-connect
list one-connect [ [ [name] | [glob] | [regex] ] ... ]
show running-config one-connect
show running-config one-connect [ [ [name] | [glob] | [regex] ] ... ]
  options:
    all-properties
    non-default-properties
    one-line
    partition
show one-connect
show one-connect [ [name] | [glob] | [regex] ] ... ]

options:
   (default | exa | gig | kil | meg | peta | raw | tera | yotta | zetta)
field-fmt
global

Delete

delete one-connect [name]

Description

You can use the one-connect component to create a OneConnect profile that optimizes connections by improving client performance and increasing server capacity.

Examples

Creates a OneConnect profile named my_OC_profile that inherits its settings from the system default OneConnect profile named oneconnect:

create one-connect my_OC_profile defaults-from oneconnect

Displays all properties for all OneConnect profiles:

list one-connect all-properties

Options

You can use the following options with the oneconnect component:

◆ defaults-from
   Specifies the profile that you want to use as the parent profile. Your new profile inherits all settings and values from the parent profile specified. The default value is oneconnect.

◆ description
   User-defined description.

◆ glob
   Displays the items that match the glob expression. For a description of glob expression syntax, see the glob man page.

◆ idle-timeout-override
   Specifies the number of seconds that a connection is idle before the connection flow is eligible for deletion. The default value is disabled.
◆ **max-age**
  Specifies the maximum age, in number of seconds, of a connection in the connection reuse pool. For any connection with an age higher than this value, the system removes that connection from the reuse pool. The default value is **86400**.

◆ **max-reuse**
  Specifies the maximum number of times that a server connection can be reused. The default value is **1000**.

◆ **max-size**
  Specifies the maximum number of connections that the system holds in the connection reuse pool. If the pool is already full, then the server connection closes after the response is completed. The default value is **10000**.

◆ **name**
  Specifies a unique name for the component. This option is required for the commands **create**, **delete**, and **modify**.

◆ **partition**
  Displays the administrative partition within which the component resides.

◆ **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. For a description of regular expression syntax, see the **regex** man page.

◆ **source-mask**
  Specifies a source IP mask. The default value is **0.0.0.0**.
  The system applies the value of this option to the source address to determine its eligibility for reuse. A mask of **0.0.0.0** causes the system to share reused connections across all clients. A host mask (all 1’s in binary), causes the system to share only those reused connections originating from the same client IP address.

### See also

radius

Configures a RADIUS profile for network traffic load balancing.

Module

ltm profile

Syntax

Configure the radius component within the ltm profile module using the following syntax.

Create/Modify

create radius [name]
modify radius [name]
   options:
      clients [add | delete | modify | replace-all-with] \ 
      ( [ip address] ... )
      clients none
      defaults-from [name]
      description [string]
      persist-avp [ [string] | [integer] | none]
edit radius [ [ [name] | [glob] | [regex] ] ... ]
   options:
      all-properties
      non-default-properties
reset-stats radius
reset-stats radius [ [ [name] | [glob] | [regex] ] ... ]

Display

list radius
list radius [ [ [name] | [glob] | [regex] ] ... ]
show running-config radius
show running-config radius [ [ [name] | [glob] | [regex] ] ... ]
   options:
      all-properties
      non-default-properties
      one-line
      partition
show radius
show radius [ [ [name] | [glob] | [regex] ] ... ]
   options:
Delete

delete radius [name]

Description

You can use the radius component to manage RADIUS network traffic.

Examples

Creates a custom RADIUS profile named my_radius_server that inherits its settings from the system default RADIUS profile:

create rtsp my_radius_server defaults-from radiusLB

Displays all properties for all RADIUS profiles:

list radius all-properties

Options

You can use these options with the radius component:

- **clients**
  Specifies host and network addresses from which clients can connect. The default value is none, which indicates that any client can connect.

- **defaults-from**
  Specifies the profile that you want to use as the parent profile. Your new profile inherits all of the settings and values from the specified parent profile. The default value is radiusLB.

- **description**
  User-defined description.

- **glob**
  Displays the items that match the glob expression. For a description of glob expression syntax, see the glob man page.

- **name**
  Specifies a unique name for the component. This option is required for the commands create, delete, and modify.

- **partition**
  Displays the administrative partition within which the component resides.
- **persist-avp**
  Specifies the name of the RADIUS attribute on which traffic persists. Acceptable values are ASCII strings from section 5 of RFC 2865 or numeric codes (1-255). The default value is `none`, which indicates that persistence is disabled.

- **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. For a description of regular expression syntax, see the `regex` man page.

**See also**

`create`, `delete`, `edit`, `glob`, `list`, `ltm virtual`, `modify`, `regex`, `reset-stats`, `show`, `tmsh`
ramcache

Manages the BIG-IP system RAM cache.

Module

ltm profile

Syntax

Configure the `ramcache` component within the `ltm profile` module using the following syntax.

Display

```
show ramcache
show ramcache [ [name] | [glob] | [regex] ] ...
```

options:

- `exact`
- `host [string]`
- `max-response [integer]`
- `uri [string]`

Delete

```
delete ramcache [name]
```

Description

You can use the `ramcache` component to delete the entries in or show information about the BIG-IP system RAM cache.

Examples

Displays information about the entries in the BIG-IP system RAM cache:
```
show ramcache
```

Deletes the entries in the BIG-IP system RAM cache:
```
delete ramcache
```
Options

You can use these options with the `ramcache` component:

- **exact**
  Displays the exact number of entries in the RAM cache.

- **host**
  Displays the host from which the entry was cached.

- **max-response**
  Displays the maximum number of entries that can be in the RAM cache.
  The default value is 0 (zero), which means that the system does not limit
  the maximum entries.

- **regex**
  Displays the items that match the regular expression. The regular
  expression must be preceded by an at sign (@[regular expression]) to
  indicate that the identifier is a regular expression. See help `regex` for a
  description of regular expression syntax.

- **uri**
  Displays the URI from which the entry was cached.

See also

delete, show, tmsh
**request-log**

Configures a Request-Logging profile.

**Module**

**ltm profile**

**Syntax**

Configure the request-log component within the ltm profile module using the syntax shown in the following sections.

**Create/Modify**

```plaintext
create request-log [name]
modify request-log [name]
  options:
    defaults-from [[name] | none]
    description [string]
    log-request-logging-errors [disabled | enabled]
    log-response-by-default [disabled | enabled]
    log-response-logging-error [disabled | enabled]
    proxy-close-on-error [disabled | enabled]
    proxy-respond-on-logging-error [disabled | enabled]
    proxy-response [string]
    request-log-error-pool [ [pool_name] | none]
    request-log-error-protocol [ TCP | UDP | none]
    request-log-error-template [string]
    request-log-pool [ [pool_name] | none]
    request-log-protocol [ TCP | UDP | none]
    request-log-template [string]
    request-logging [disabled | enabled]
    response-log-error-pool [ [pool_name] | none]
    response-log-error-protocol [ TCP | UDP | none]
    response-log-error-template [string]
    response-log-pool [ [pool_name] | none]
    response-log-protocol [ TCP | UDP | none]
    response-log-template [string]
    response-logging [disabled | enabled]

edit request-log [ [ [name] | [glob] | [regex] ] ... ]
  options:
    all-properties
    non-default-properties
```
Display

list request-log
list request-log [ [ [name] | [glob] | [regex] ] ... ]
show running-config request-log
show running-config request-log
  [ [ [name] | [glob] | [regex] ] ... ]
options:
  all-properties
  non-default-properties
  one-line
  partition
show request-log
show request-log [ [ [name] | [glob] | [regex] ] ... ]
options:
  (default | exa | gig | kil | meg | peta | raw | tera | yotta | zetta)
  field-fmt
  global

Delete

delete request-log [name]

Description

You can use the request-log component to manage request log network traffic.

Examples

Creates a custom request-log profile named my_request-log_profile that inherits its settings from the system default request-log profile:

create request-log my_request-log_profile defaults-from request-logging

Displays all properties for all request-log profiles:
list request-log all-properties

Options

You can use these options with the request-log component:

- defaults-from
  Specifies the default values from this profile.

- description
  User-defined description.
◆ **log-request-logging-errors**
Enables secondary logging should the primary lack sufficient available bandwidth. This mechanism is best used to send an alert to a completely separate destination.

◆ **log-response-by-default**
Indicates if response logging can be overridden using iRules® or httpclass. This field determines the default response action.

◆ **log-response-logging-errors**
Enables secondary logging should the primary lack sufficient available bandwidth. This mechanism is best used to send an alert to a completely separate destination.

◆ **partition**
Displays the administrative partition within which the profile resides.

◆ **proxy-close-on-error**
Specifies that, if enabled, the logging profile will close the connection after sending its proxy-response.

◆ **proxy-respond-on-logging-error**
Specifies that the logging profile respond directly (for example, with an HTTP 502) if the logging fails.

◆ **proxy-response**
Specifies the response to send on logging errors.

◆ **regex**
Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. See help regex for a description of regular expression syntax.

◆ **request-log-error-pool**
Specifies the name of the pool from which to select log servers.

◆ **request-log-error-protocol**
Specifies the HighSpeedLogging protocol to use when logging.

◆ **request-log-error-template**
Specifies the template to use when generating log messages. Shell style escapes (eg $foo and/or ${foo}) are used to import transaction-specific values.

◆ **request-log-pool**
Specifies the name of the pool from which to select log servers.

◆ **request-log-protocol**
Specifies the HighSpeedLogging protocol to use when logging.

◆ **request-log-template**
Specifies the template to use when generating log messages. Shell style escapes (eg $foo and/or ${foo}) are used to import transaction-specific values.

◆ **request-logging**
Enables or disables logging before the response is returned to the client.

◆ **response-log-error-pool**
Specifies the name of the pool from which to select log servers.
◆ **response-log-error-protocol**  
Specifies the HighSpeedLogging protocol to use when logging.

◆ **response-log-error-template**  
Specifies the template to use when generating log messages. Shell style escapes (eg $foo and/or ${foo}) are used to import transaction-specific values.

◆ **response-log-pool**  
Specifies the name of the pool from which to select log servers.

◆ **response-log-protocol**  
Specifies the HighSpeedLogging protocol to use when logging.

◆ **response-log-template**  
Specifies the template to use when generating log messages. Shell style escapes (eg $foo and/or ${foo}) are used to import transaction-specific values.

◆ **response-logging**  
Enables or disables logging before the response is returned to the client.

**See also**

create, delete, edit, glob, ltm profile, ltm virtual, modify, show, regex, tmsh
rtsp

Configures a Real Time Streaming Protocol (RTSP) profile.

Module

ltm profile

Syntax

Configure the rtsp component within the ltm profile module using the following syntax.

Create/Modify

create rtsp [name]
modify rtsp [name]

options:
  check-source [disabled | enabled]
  defaults-from [name]
  description [string]
  idle-timeout [integer]
  max-header-size [integer]
  max-queued-data [integer]
  multicast-redirect [disabled | enabled]
  proxy [external | internal | none]
  proxy-header [ [name] | none]
  real-http-persistence [disabled | enabled]
  rtcp-port [number]
  rtp-port [number]
  session-reconnect [disabled | enabled]
  unicast-redirect [disabled | enabled]

edit rtsp [ [ [name] | [glob] | [regex] ] ... ]

options:
  all-properties
  non-default-properties
reset-stats rtsp
reset-stats rtsp [ [ [name] | [glob] | [regex] ] ... ]

Display

list rtsp
list rtsp [ [ [name] | [glob] | [regex] ] ... ]
show running-config rtsp
show running-config rtsp [ [ [name] | [glob] | [regex] ] ... ]
  options:
    all-properties
    non-default-properties
    one-line
    partition
show rtsp
show rtsp [ [ [name] | [glob] | [regex] ] ... ]
  options:
    (default | exa | gig | kil | meg | peta | raw | tera | yotta | zetta)
    field-fmt
    global

Delete

delte rtsp [name]

Description

You can use the rtsp component to manage a profile that you use to control RTSP traffic.

Examples

Creates a custom RTSP profile named my_rtsp_profile that inherits its settings from the system default RTSP profile:
create rtsp my_rtsp_profile defaults-from rtsp

Displays all properties for all RTSP profiles:
list rtsp all-properties

Options

You can use these options with the rtsp component:

- **check-source**
  When enabled the system uses the source attribute in the transport header to establish the target address of the RTP stream, and before the response is forwarded to the client, updates the value of the source attribute to be the virtual address of the BIG-IP system. When disabled the system does not change the source attribute. The default value is enabled.

- **defaults-from**
  Specifies the profile that you want to use as the parent profile. Your new profile inherits all of the settings and values from the specified parent profile. The default value is rtsp.
◆ **description**  
User-defined description.

◆ **glob**  
Displays the items that match the glob expression. For a description of glob expression syntax, see the glob man page.

◆ **idle-timeout**  
Specifies the number of seconds that a connection is idle before the connection is eligible for deletion. The default value is **300** seconds.

◆ **max-header-size**  
Specifies the maximum size of an RTSP request or response header that the RTSP filter accepts before dropping the connection. The default value is **4096** bytes.

◆ **max-queued-data**  
Specifies the maximum amount of data that the RTSP filter buffers before dropping the connection. The default value is **32768** bytes.

◆ **multicast-redirect**  
Specifies whether to enable or disable multicast redirect. When enabled, the client can select the destination to which to stream data. The default value is **disabled**.

◆ **name**  
Specifies a unique name for the component. This option is required for the commands **create**, **delete**, and **modify**.

◆ **partition**  
Displays the administrative partition within which the component resides.

◆ **proxy**  
Specifies whether the RTSP filter is associated with an RTSP proxy configuration. The default value is **none**.

◆ **proxy-header**  
When the **proxy** option is set, specifies the name of the header in the RTSP proxy configuration that is passed from the client-side virtual server to the server-side virtual server. The name of the header must begin with **X-**. The default value is **none**.

To use the **proxy-header** option, you must specify a value for the **proxy** option.

◆ **real-http-persistence**  
Specifies whether to enable or disable real HTTP persistence. When enabled, the RTSP filter automatically persists Real Networks RTSP over HTTP using the RTSP port. The default value is **enabled**. If you disable this parameter, you can override the default behavior with an iRule.

◆ **regex**  
Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. For a description of regular expression syntax, see the regex man page.
◆ **rtp-port**
Specifies the number of the port to use for the RTP service. The default value is 0 (zero).

◆ **rtp-port**
Specifies the number of the port to use for the RTP service. The default value is 0 (zero).

◆ **session-reconnect**
Specifies whether to enable or disable session reconnect. When enabled, the RTSP filter persists the control connection, which is being resumed, to the correct server. The default value is disabled.

◆ **unicast-redirect**
Specifies whether to enable or disable unicast redirect. When enabled, the client can select the destination to which to stream data. The default value is disabled.

See also

create, delete, edit, glob, list, ltm virtual, modify, regex, reset-stats, show, tmsh
sctp

Configures a Stream Control Transmission Protocol (SCTP) profile.

Module

ltm profile

Syntax

Configure the sctp component within the ltm profile module using the following syntax.

Create/Modify

create sctp [name]
modify sctp [name]

options:
  cookie-expiration [integer]
  defaults-from [name]
  description [string]
  heartbeat-interval [integer]
  idle-timeout [integer]
  in-streams [integer]
  init-max-retries [integer]
  ip-tos [integer]
  link-qos [integer]
  out-streams [integer]
  proxy-buffer-high [integer]
  proxy-buffer-low [integer]
  receive-chunks [integer]
  receive-ordered [disabled | enabled]
  receive-window-size [integer]
  reset-on-timeout [disabled | enabled]
  secret [default | [string] ]
  send-buffer-size [integer]
  send-max-retries [integer]
  send-partial [disabled | enabled]
  tcp-shutdown [disabled | enabled]
  transmit-chunks [integer]

edit sctp [ [ [name] | [glob] | [regex] ] ... ]

options:
  all-properties
  non-default-properties
reset-stats sctp
reset-stats sctp [ [name] | [glob] | [regex] ] ... 

Display

list sctp
list sctp [ [name] | [glob] | [regex] ] ... 
show running-config sctp
show running-config sctp [ [name] | [glob] | [regex] ] ... 
options:
  all-properties
  non-default-properties
  one-line
  partition

show sctp
show sctp [ [name] | [glob] | [regex] ] ... 
options:
  (default | exa | gig | kil | meg | peta | raw | tera | yotta | zetta)
  field-fmt
  global

Delete

delete sctp [name]

Description

You can use the sctp component to manage a profile for SCTP traffic.

Examples

Creates a custom SCTP profile named my_sctp_profile that inherits its settings from the system default SCTP profile:
create sctp my_sctp_profile defaults-from sctp

Displays all properties for all SCTP profiles:
list sctp all-properties

Options

You can use these options with the sctp component:

- **cookie-expiration**
  Specifies how many seconds the cookie is valid. The default value is 60 seconds.
- **description**
  User-defined description.

- **defaults-from**
  Specifies the profile that you want to use as the parent profile. Your new profile inherits all settings and values from the parent profile specified. The default value is `sctp`.

- **glob**
  Displays the items that match the `glob` expression. For a description of `glob` expression syntax, see the `glob` man page.

- **heartbeat-interval**
  Specifies the number of seconds to wait before sending a heartbeat chunk. The default value is 30 seconds.

- **idle-timeout**
  Specifies the number of seconds without traffic before a connection is eligible for deletion. The default value is 300 seconds.

- **in-streams**
  Specifies the number of inbound streams. The default value is 2.

- **init-max-retries**
  Specifies the maximum number of retries to establish a connection. The default value is 4.

- **ip-tos**
  Specifies the Type of Service (ToS) that is set in the packets sent to the peer. The default value is 0.

- **link-qos**
  Specifies the Link Quality of Service (QoS) that is set in sent packets. The default value is 0 (zero).

- **name**
  Specifies a unique name for the component. This option is required for the commands `create`, `delete`, and `modify`.

- **out-streams**
  Specifies the number of outbound streams. The default value is 2.

- **partition**
  Displays the administrative partition within which the component resides.

- **proxy-buffer-high**
  Specifies the proxy buffer level after which the system closes the receive window. The default value is 16384.

- **proxy-buffer-low**
  Specifies the proxy buffer level after which the system opens the receive window. The default value is 4096.

- **receive-chunks**
  Specifies the size (in chunks) of the `rx_chunk` buffer. The default value is 256.

- **receive-ordered**
  When enabled, the default, the system delivers messages to the application layer in order.
- **receive-window-size**
  Specifies the size (in bytes) of the receive window. Prorate this value to the receive-chunks value. The default value is 65536.

- **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. For a description of regular expression syntax, see the regex man page.

- **reset-on-timeout**
  When enabled, the default, the system resets a connection when the connection times out.

- **secret**
  Specifies the internal secret string that the system uses for HTTP Message Authenticated Code (HMAC) cookies.

- **send-buffer-size**
  Specifies the size in bytes of the buffer. The default value is 65536.

- **send-max-retries**
  Specifies the maximum number of times the system tries again to send data. The default value is 8.

- **send-partial**
  When enabled, the default, the system accepts partial application data.

- **tcp-shutdown**
  When enabled, the system emulates the closing of a TCP connection. The default value is enabled.

- **transmit-chunks**
  Specifies the size (in chunks) of the tx_chunk buffer. The default value is 256.

**See also**

create, delete, edit, glob, list, ltm virtual, modify, regex, reset-stats, show, tmsh
server-ssl

Configures a Server SSL profile.

Module

ltm profile

Syntax

Configure the server-ssl component within the ltm profile module using the following syntax.

Create/Modify

create server-ssl [name]
modify server-ssl [name]

options:
    alert-timeout [indefinite | [integer] ]
    authenticate [always | once]
    authenticate-depth [integer]
    authenticate-name [ [name] | none]
    ca-file [ [file name] | none]
    cache-size [integer]
    cache-timeout [integer]
    cert [ [file name] | none]
    chain [ [name] | none]
    ciphers [ [name] | none]
    crl-file [none]
    defaults-from [ [name] | none]
    description [string]
    handshake-timeout [indefinite | [integer] ]
    key [ [file name] | none]
    mod-ssl-methods [disabled | enabled]
    mode [disabled | enabled]

    options { none | [ all-bugfixes cipher-server-preference dont-insert-empty-fragments \ 
                  ephemeral-rsa microsoft-big-sslv3-buffer microsoft-sess-id-bug \ 
                  msie-sslv2-rsa-padding netscape-ca-cn-bug netscape-challenge-bug \ 
                  netscape-demo-cipher-change-bug netscape-reuse-cipher-change-bug \ 
                  no-session-resumption-on-renegotiation no-sslv2 no-sslv3 no-tls1 \ 
                  passive-close pkcs1-check-1 pkcs1-check-2 single-dh-use \ 
                  ssleay-080-client-dh-bug sslref2-reuse-cert-type-bug tls-block-padding-bug \ 
                  tls-d5-bug tls-rollback-bug] }
    passphrase [none | [string] ]
    peer-cert-mode [ignore | require]
    proxy-ssl [disabled | enabled]
You can use the `server-ssl` component to manage a Server SSL profile. Server-side profiles enable the traffic management system to handle encryption tasks for any SSL connection being sent from a Local Traffic Manager system to a target server. A server-side SSL profile acts as a client by presenting certificate credentials to a server when authentication of the Local Traffic Manager system is required. You implement this type of profile by using the default profile or by creating a custom profile based on the Server SSL profile template and modifying its settings.
Examples

Creates a custom Server SSL profile named `my_serverssl_profile` that inherits its settings from the system default `serverssl` profile:
```
create serverssl my_serverssl_profile defaults-from serverssl
```

Displays all properties for all Server SSL profiles:
```
list server-ssl all-properties
```

Options

You can use these options with the `server-ssl` component:

- **alert-timeout**
  Specifies the alert timeout in seconds. The default value is **60** seconds.

- **authenticate**
  Specifies the frequency of authentication. The default value is **once**.

- **authenticate-depth**
  Specifies the client certificate chain maximum traversal depth. The default value is **9**.

- **authenticate-name**
  Specifies a Common Name (CN) that is embedded in a server certificate. The system authenticates a server based on the specified CN. The default value is **none**.

- **ca-file**
  Specifies the certificate authority (CA) file name. Configures certificate verification by specifying a list of client or server CAs that the traffic management system trusts. The default value is **none**.

- **cache-size**
  Specifies the SSL session cache size. For client profiles only, you can configure timeout and size values for the SSL session cache. Because each profile maintains a separate SSL session cache, you can configure the values on a per-profile basis. The default value is **20000**.

- **cache-timeout**
  Specifies the SSL session cache timeout value, which is the usable lifetime seconds of negotiated SSL session IDs. The default value is **3600** seconds. Acceptable values are integers greater than or equal to **0** and less than or equal to **86400**.

- **cert**
  Specifies the name of the certificate installed on the traffic management system for the purpose of terminating or initiating an SSL connection. The default value is **none**.

- **chain**
  Specifies or builds a certificate chain file that a client can use to authenticate the profile. The default value is **none**.

- **ciphers**
  Specifies a cipher name. The default value is **DEFAULTS**.
- **crl-file**
  Specifies the certificate revocation list file name. The default value is `none`.
- **defaults-from**
  Specifies the profile that you want to use as the parent profile. Your new profile inherits all settings and values from the parent profile specified. The default value is `serverssl`.
- **description**
  User-defined description.
- **glob**
  Displays the items that match the `glob` expression. For a description of `glob` expression syntax, see the `glob` man page.
- **handshake-timeout**
  Specifies the handshake timeout in seconds. The default value is `60`.
- **key**
  Specifies the key file name. Specifies the name of the key installed on the traffic management system for the purpose of terminating or initiating an SSL connection. The default value is `none`.
- **mod-ssl-methods**
  Enables or disables ModSSL method emulation. The default value is `disabled`.
  Enable this option when OpenSSL methods are inadequate. For example, you can enable ModSSL method emulation when you want to use SSL compression over TLSv1.
- **mode**
  Enables or disables SSL processing. The default value is `enabled`.
- **name**
  Specifies a unique name for the component. This option is required for the commands `create`, `delete`, and `modify`.
- **options**
  Enables options, including some industry-related workarounds. Enter options inside braces, for example: `{dont-insert-empty-fragments microsoft-sess-id-bug}`. The default value is `dont-insert-empty-fragments`.
  The options are:
  - **all-bugfixes**
    This option enables the following industry-related defect workarounds: `microsoft-sess-id-bug`, `netscape-challenge-bug`, `netscape-reuse-cipher-change-bug`, `ssleay2-reuse-cert-type-bug`, `microsoft-big-sslv3-buffer`, `msie-sslv2-rsa-padding`, `ssleay-080-client-dh-bug`, `tls-d5-bug`, `tls-block-padding-bug`, and `dont-insert-empty-fragments`. It is usually safe to use this option to enable the defect workaround options when compatibility with broken implementations is required. If you edit the configuration in the browser-based Configuration utility, the system expands the `all-bugfixes` syntax into each individual option.
• **cipher-server-preference**
  When choosing a cipher, the server uses either the server preferences or the client references. When this option is not set, the SSL server always follows the client references. When this option is set, the SSLv3/TLSv1 server chooses by using its own references. Due to the different protocol, for SSLv2 the server sends its list of preferences to the client and the client always chooses.

• **dont-insert-empty-fragments**
  Disables a countermeasure against an SSL 3.0/TLS 1.0 protocol vulnerability affecting CBC ciphers. These ciphers cannot be handled by certain broken SSL implementations. This option has no effect for connections using other ciphers.

• **ephemeral-rsa**
  Uses ephemeral (temporary) RSA keys for RSA operations. According to the specifications, SSL uses ephemeral RSA keys only for signature operations (namely under export ciphers with restricted RSA key length). By setting this option, you specify that you always want SSL to always use ephemeral RSA keys. This option breaks compatibility with the SSL/TLS specifications and can lead to interoperability problems with clients. Therefore, F5 Networks does not recommend this option. Use ciphers with EDH (ephemeral Diffie-Hellman) key exchange instead. This option is ignored for server-side SSL.

• **microsoft-big-sslv3-buffer**
  Enables a workaround for communicating with older Microsoft applications that use non-standard SSL record sizes.

• **microsoft-sess-id-bug**
  Handles a Microsoft session ID problem.

• **msie-sslv2-rsa-padding**
  Enables a workaround for communicating with older Microsoft applications that use non-standard RSA key padding. This option is ignored for server-side SSL.

• **netscape-ca-dn-bug**
  Handles a defect regarding the system crashing or hanging. If the system accepts a Netscape Navigator browser connection, demands a client cert, has a non-self-signed CA that does not have its CA in Netscape, and the browser has a certificate, the system crashes or hangs.

• **netscape-challenge-bug**
  Handles the Netscape challenge problem.

• **netscape-demo-cipher-change-bug**
  Manipulates the SSL server session resumption behavior to mimic that of certain Netscape servers (see the Netscape reuse cipher change bug workaround description). F5 Networks does not recommend this option for normal use. It is ignored for server-side SSL.
• **netscape-reuse-cipher-change-bug**
   Handles a defect within Netscape-Enterprise/2.01, appearing only when connecting through SSLv2/v3, and then reconnecting through SSLv3. In this case, the cipher list changes. First, Netscape establishes a connection with the RC4-MD5 cipher list. If the connection is resumed, Netscape switches to using the DES-CBC3-SHA cipher list. However, according to RFC 2246, section 7.4.1.3, cipher suite) the cipher list is RC4-MD5. As a workaround, you can set Netscape to attempt to connect with a cipher list of DES-CBC-SHA:RC4-MD5, and so on. For some reason, each new connection uses the RC4-MD5 cipher list, but any re-connection attempts to use the DES-CBC-SHA cipher list. Thus Netscape, when reconnecting, always uses the first cipher in the cipher list.

• **no-session-resumption-on-renegotiation**
   When an SSL server performs renegotiation, this option always starts a new session (that is, session resumption requests are accepted only in the initial handshake). The system ignores this option for server-side SSL.

• **no-sslv2**
   Do not use the SSLv2 protocol.

• **no-sslv3**
   Do not use the SSLv3 protocol.

• **no-tlsv1**
   Do not use the TLSv1 protocol.

• **passive-close**
   Specifies how to handle passive closes.

• **none**
   Disables all workarounds. F5 Networks does not recommend this option.

• **pkcs1-check-1**
   This debugging option deliberately manipulates the PKCS1 padding used by SSL clients in an attempt to detect vulnerability to particular SSL server vulnerabilities. F5 Networks does not recommend this option for normal use. The system ignores this option for client-side SSL.

• **pkcs1-check-2**
   This debugging option deliberately manipulates the PKCS1 padding used by SSL clients in an attempt to detect vulnerability to particular SSL server vulnerabilities. F5 Networks does not recommend this option for normal use. The system ignores this option for client-side SSL.

• **single-dh-use**
   Creates a new key when using temporary/ephemeral DH parameters. This option must be used to prevent small subgroup attacks, when the DH parameters were not generated using strong primes (for example, when using DSA-parameters). If strong primes were used, it is not
strictly necessary to generate a new DH key during each handshake, but F5 Networks recommends it. Enable the `single-dh-use` option whenever temporary or ephemeral DH parameters are used.

- **ssleay-080-client-dh-bug**  
  Enables a workaround for communicating with older SSLeay-based applications that specify an incorrect Diffie-Hellman public value length. This option is ignored for server-side SSL.

- **sslref2-reuse-cert-type-bug**  
  Handles the SSL reuse certificate type problem.

- **tls-block-padding-bug**  
  Enables a workaround for communicating with older TLSv1-enabled applications that use incorrect block padding.

- **tls-d5-bug**  
  This option is a workaround for communicating with older TLSv1-enabled applications that specify an incorrect encrypted RSA key length. This option is ignored for server-side SSL.

- **tls-rollback-bug**  
  Disables version rollback attack detection. During the client key exchange, the client must send the same information about acceptable SSL/TLS protocol levels as it sends during the first hello. Some clients violate this rule by adapting to the server's answer. For example, the client sends an SSLv2 hello and accepts up to SSLv3.1 (TLSv1), but the server processes only up to SSLv3. In this case, the client must still use the same SSLv3.1 (TLSv1) announcement. Some clients step down to SSLv3 with respect to the server's answer and violate the version rollback protection. The system ignores this option for server-side SSL.

- **partition**  
  Displays the administrative partition within which the component resides.

- **passphrase**  
  Specifies the key passphrase, if required. The default value is `none`.

- **peer-cert-mode**  
  Specifies the peer certificate mode. The default value is `ignore`.

- **proxy-ssl**  
  Enabling this option requires a corresponding client ssl profile with `proxy-ssl` enabled to perform transparent SSL decryption. This feature allows further modification of application traffic within an SSL tunnel while still allowing the server to perform necessary authorization, authentication, auditing steps.

- **regex**  
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (`@[regular expression]`) to indicate that the identifier is a regular expression. For a description of regular expression syntax, see the `regex` man page.
◆ **renegotiate-period**
Specifies the number of seconds from the initial connect time after which the system renegotiates an SSL session. The default value is **indefinite**, which means that you do not want the system to renegotiate SSL sessions.

Each time the session renegotiation is successful, a new connection is started. Therefore, the system attempts to renegotiate the session again, in the specified amount of time following a successful session renegotiation. For example, setting the **renegotiate-period** option to **3600** seconds triggers session renegotiation at least once an hour.

◆ **renegotiate-size**
Specifies a throughput size, in megabytes, of SSL renegotiation. This option forces the traffic management system to renegotiate an SSL session based on the size, in megabytes, of application data that is transmitted over the secure channel. The default value is **indefinite**, which specifies that you do not want a throughput size.

◆ **renegotiation**
Enables or disables renegotiation. The default value is **enabled**.

When renegotiations are disabled, the system is acting as an SSL server, and a COMPAT or NATIVE cipher is negotiated, the system aborts the connection. Additionally, when renegotiations are disabled and the system is acting as an SSL client, the system ignores the server's HelloRequest messages.

◆ **strict-resume**
Enables or disables the resumption of SSL sessions after an unclean shutdown. The default value is **disabled**, which indicates that the SSL profile refuses to resume SSL sessions after an unclean shutdown.

◆ **unclean-shutdown**
Specifies, when enabled, that the SSL profile performs unclean shutdowns of all SSL connections, which means that underlying TCP connections are closed without exchanging the required SSL shutdown alerts. If you want to force the SSL profile to perform a clean shutdown of all SSL connections, you can disable this option.

**See also**

create, delete, edit, glob, list, ltm profile client-ssl, ltm virtual, modify, regex, show, tmsh
**sip**

Configures a Session Initiation Protocol (SIP) profile.

**Module**

**ltm profile**

**Syntax**

Configure the **sip** component within the **ltm profile** module using the following syntax.

**Create/Modify**

```
create sip [name]
modify sip [name]
```

```
options:
  community [ [community name] | none]
  defaults-from [ [name] | none]
  description [string]
  dialog-aware [disabled | enabled]
  insert-record-route-header [disabled | enabled]
  insert-via-header [disabled | enabled]
  max-size [integer]
  secure-via-header [disabled | enabled]
  security [disabled | enabled]
  terminate-on-bye [disabled | enabled]
  user-via-header [ [via-header] | none]
```

```
edit sip [ [ [name] | [glob] | [regex] ] ... ]
```

```
options:
  all-properties
  non-default-properties
reset-stats sip
reset-stats sip [ [ [name] | [glob] | [regex] ] ... ]
```

**Display**

```
list sip
list sip [ [ [name] | [glob] | [regex] ] ... ]
show running-config sip
show running-config sip [ [ [name] | [glob] | [regex] ] ... ]
```

```
options:
  all-properties
```
non-default-properties
one-line
partition
show sip
show sip [ [ name ] | [ glob ] | [ regex ] ] ...
    options:
        (default | exa | gig | kil | meg | peta | raw | tera | yotta | zetta)
    field-fmt

Delete

    delete sip [ name ]

Description

You can use the **sip** component to manage a SIP profile.

Examples

Creates a SIP profile named **my_sip_profile** using the system defaults:

```
create sip my_sip_profile defaults-from sip
```

Creates a SIP profile named **my_sip_profile** that leaves a connection open following the completion of a BYE transaction:

```
create sip my_sip_profile { terminate-bye disabled }
```

Options

You can use the following options with the **sip** component:

- **community**
  Specifies the community to which you want to assign the virtual server that you associate with this profile. The default value is **none**.

- **defaults-from**
  Specifies the profile that you want to use as the parent profile. Your new profile inherits all of the settings and values from the specified parent profile. The default value is **sip**.

- **description**
  User-defined description.

- **dialog-aware**
  Enables or disables the ability for the system to be aware of unauthorized use of the SIP dialog. The default value is **disabled**.

- **glob**
  Displays the items that match the **glob** expression. For a description of **glob** expression syntax, see the **glob** man page.
◆ **insert-record-route-header**
Enables or disables the insertion of a Record-Route header, which indicates the next hop for the following SIP request messages. The default value is **disabled**.

◆ **insert-via-header**
Enables or disables the insertion of a Via header, which indicates where the message originated. The response message uses this routing information. The default value is **disabled**.

◆ **max-size**
Specifies the maximum SIP message size that the BIG-IP system accepts. The default value is **65535** bytes.

◆ **name**
Specifies a unique name for the component. This option is required for the commands **create**, **delete**, and **modify**.

◆ **partition**
Displays the administrative partition within which the component resides.

◆ **regex**
Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. For a description of regular expression syntax, see the **regex** man page.

◆ **secure-via-header**
Enables or disables the insertion of a Secure Via header, which indicates where the message originated. When you are using SSL/TLS (over TCP) to create a secure channel with the server node, use this option to configure the system to insert a Secure Via header into SIP requests. The default value is **disabled**.

◆ **security**
Enables or disables security for the SIP profile. The default value is **disabled**.

◆ **terminate-on-bye**
Enables or disables the termination of a connection when a BYE transaction finishes. Use this parameter with UDP connections only, not with TCP connections. The default value is **enabled**.

◆ **user-via-header**
Enables or disables the insertion of a Via header specified by a system administrator. The default value is **none**.

---

**See also**

create, delete, edit, glob, list, ltm virtual, modify, regex, reset-stats, show, tmsh
smtp

Configures a Session Initiation Protocol (SIP) profile.

Module

ltm profile

Syntax

Configure the sip component within the ltm profile module using the following syntax. The smtp profile is available when the psm module is enabled. You enable the psm module via provisioning commands, which are described in help sys provision.

Create/Modify

create smtp [name]
modify smtp [name]
  options:
    defaults-from [ [name] | none]
    description [string]
    security [disabled | enabled]
edit smtp [ [ [name] | [glob] | [regex] ] ... ]
  options:
    all-properties
    non-default-properties

Display

list smtp
list smtp [ [ [name] | [glob] | [regex] ] ... ]
show running-config smtp
show running-config smtp [ [ [name] | [glob] | [regex] ] ... ]
  options:
    all-properties
    non-default-properties

Delete

delete smtp [name]
Chapter 33

Description

You can use the `smtp` component to create, modify, display, or delete an SMTP profile with which you can manage SMTP traffic.

Examples

Creates a custom SMTP profile named `my_smtp_profile` that inherits its settings from the system default SMTP profile:

```
create smtp my_smtp_profile defaults-from smtp
```

Displays the properties of all SMTP profiles:

```
list smtp
```

Options

You can use the following options with the `smtp` component:

- **defaults-from**
  Specifies the profile that you want to use as the parent profile. Your new profile inherits all of the settings and values from the specified parent profile. The default value is `smtp`.

- **description**
  User-defined description.

- **glob**
  Displays the items that match the `glob` expression. For a description of `glob` expression syntax, see the `glob` man page.

- **name**
  Specifies a unique name for the component. This option is required for the commands `create`, `delete`, and `modify`.

- **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. For a description of regular expression syntax, see the `regex` man page.

- **security**
  Enables or disables secure SMTP traffic for the BIG-IP Application Security Manager. The default value is `disabled`.

See also

```
create, delete, edit, glob, list, ltm virtual, modify, regex, reset-stats, show, tmsh
```
**spdy**

Configures a SPDY profile.

**Module**

**ltm profile**

**Syntax**

Configure the `spdy` component within the `ltm profile` module using the following syntax.

**Create/Modify**

```
create spdy [name]
modify spdy [name]
  options:
    activation-mode [npn | always]
    concurrent-streams-per-connection [integer]
    connection-idle-timeout [integer]
    defaults-from [ [name] | none]
    description [string]
    insert-header [disabled | enabled]
    insert-header-name ["string"]
```

**Display**

```
list spdy
list spdy [ [ [name] | [glob] | [regex] ] ... ]
show running-config http
show running-config http [ [ [name] | [glob] | [regex] ] ... ]
  options:
    all-properties
    non-default-properties
    one-line
    partition
show spdy
show spdy [ [ [name] | [glob] | [regex] ] ... ]
  options:
    (default | exa | gig | kil | meg | peta | raw | tera | yotta | zetta)
    field-fmt
    global
```
Delete

delete spdy [name]

Description

You can use the spdy component to create, modify, display, or delete a SPDY profile.

The BIG-IP® system installation includes the following default SPDY-type profile:

- **spdy**
  The default SPDY profile contains values for properties related to managing SPDY traffic.
  You can create a new SPDY-type profile using an existing profile as a parent profile, and then you can change the values of the properties to suit your needs.

Examples

create spdy my_spdy_profile defaults-from spdy

Options

- **activation-mode**
  Specifies what will cause a connection to be treated as a SPDY connection. The value npn specifies that the TLS next-protocol-negotiation will be used to determine whether SPDY should be activated. Clients that use TLS, but only support HTTP will work as if SPDY is not present. The value always specifies that all connections are assumed to be SPDY connections. Clients that support only HTTP will not be able to send requests. The default value is npn.

- **concurrent-streams-per-connection**
  Specifies how many concurrent requests are allowed to be outstanding on a single SPDY connection.

- **connection-idle-timeout**
  Specifies how many seconds a SPDY connection is left open idly before it is shut down.

- **defaults-from**
  Specifies the profile that you want to use as the parent profile. Your new profile inherits all settings and values from the parent profile specified. The default value is none.

- **description**
  User defined description.
◆ **glob**
Displays the items that match the `glob` expression. See `help glob` for a description of `glob` expression syntax.

◆ **insert-header**
Specifies whether an HTTP header that indicates the use of SPDY should be inserted in the request going to the back-end server. The default value is `disabled`.

◆ **insert-header-name**
Specifies the name of the HTTP header controlled by `insert-header`. The default value is "X-SPDY".

◆ **name**
Specifies a unique name for the component. This option is required for the commands `create`, `delete`, and `modify`.

◆ **regex**
Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@ [regular expression]) to indicate that the identifier is a regular expression. See `help regex` for a description of regular expression syntax.

**See Also**

`create`, `delete`, `edit`, `glob`, `list`, `ltm profile fasthttp`, `ltm virtual`, `modify`, `regex`, `reset-stats`, `show`, `tmsh`
statistics

Configures a Statistics profile.

Module

ltm profile

Syntax

Configure the statistics component within the ltm profile module using the following syntax.

Create/Modify

create statistics [name]
modify statistics [name]

options:
  defaults-from [ [name] | none]
description [string]
field1 [string]
field2 [string]
field3 [string]
field4 [string]
field5 [string]
field6 [string]
field7 [string]
field8 [string]
field9 [string]
field10 [string]
field11 [string]
field12 [string]
field13 [string]
field14 [string]
field15 [string]
field16 [string]
field17 [string]
field18 [string]
field19 [string]
field20 [string]
field21 [string]
field22 [string]
field23 [string]
field24 [string]
You can use the statistics component to create, modify, display, or delete a Statistics profile that provides user-defined statistical counters.
Examples

Creates a Statistics profile name `my_stats_profile` that inherits all settings and values from the profile `stats`:

```bash
create statistics my_stats_profile defaults-from stats
```

Displays the configuration of the profile `my_stats_profile`:

```bash
list statistics my_stats_profile
```

Creates a Statistics profile named `my_stats_profile` with a total users counter in Field 1 and a current users counter in Field 2. You can then write an iRule to count the total number of connections and record the current number of connections:

```bash
list statistics my_stats_profile field1 total_users field2 current_users field3 max_users
```

For more information about writing and using iRules®, see the F5 Networks Dev Central web site.

Options

You can use these options with the `statistics` component:

- **defaults-from**
  Specifies the profile that you want to use as the parent profile. Your new profile inherits all settings and values from the parent profile specified. The default value is `stats`.

- **description**
  User-defined description.

- **field1 - field 32**
  Specifies the name of a counter. You can specify a counter for up to 32 fields. The default value for each field is `none`. You can then write an iRule that uses the counter names to gather statistics about the traffic the system is processing.

- **glob**
  Displays the items that match the `glob` expression. For a description of `glob` expression syntax, see the `glob` man page.

- **name**
  Specifies a unique name for the component. This option is required for the commands `create`, `delete`, and `modify`.

- **partition**
  Displays the administrative partition within which the component resides.

- **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. For a description of regular expression syntax, see the `regex` man page.
See also

create, delete, edit, glob, list, ltm virtual, modify, regex, reset-stats, show, tmsh
stream

Configures a Stream profile.

Module

ltm profile

Syntax

Configure the stream component within the ltm profile module using the following syntax.

Create/Modify

create stream [name]
modify stream [name]
options:
  defaults-from [ [name] | none]
  source [none | [string]]
  target [none | [string]]
edit stream [ [ [name] | [glob] | [regex] ] ... ]
options:
  all-properties
  non-default-properties
reset-stats stream
reset-stats stream [ [ [name] | [glob] | [regex] ] ... ]

Display

list stream
list stream [ [ [name] | [glob] | [regex] ] ... ]
show running-config stream
show running-config stream [ [ [name] | [glob] | [regex] ] ... ]
options:
  all-properties
  non-default-properties
  one-line
  partition
show stream
show stream [ [ [name] | [glob] | [regex] ] ... ]
options:
  (default | exa | gig | kil | meg | peta | raw | tera | yotta | zetta)
field-fmt
  global

Delete

    delete stream [name]

Description

You can use the stream component to search and replace strings within a data stream, such as a TCP connection.

Examples

Creates a custom Stream profile named my_stream_profile that inherits its settings from the system default stream profile:

    create stream my_stream_profile defaults-from stream

Displays all properties for all Stream profiles:

    list stream all-properties

Options

You can use these options with the stream component:

- **defaults-from**
  Specifies the profile that you want to use as the parent profile. Your new profile inherits all settings and values from the parent profile specified. The default value is stream.

- **description**
  User-defined description.

- **glob**
  Displays the items that match the glob expression. For a description of glob expression syntax, see the glob man page.

- **name**
  Specifies a unique name for the component. This option is required for the commands create, delete, and modify.

- **partition**
  Displays the administrative partition within which the component resides.

- **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. For a description of regular expression syntax, see the regex man page.
Source
Specifies the string that the system uses to rewrite the target string. The default value is **none**.

Target
Specifies the string you want to rewrite. The default value is **none**.

See also

create, delete, edit, glob, list, ltm virtual, modify, regex, reset-stats, show, tmsh
**tce**

Configures a Traffic Control and Enforcement (TCE) profile.

**Module**

ltm profile

**Syntax**

Configure the tce component within the ltm profile module using the following syntax.

**Create/Modify**

```
create tce [name]
modify tce [name]
  options:
    description [string]
    policy [none | [name] ]
edit tce [ [ [name] | [glob] | [regex] ] ... ]
  options:
    all-properties
    non-default-properties
reset-stats tce
reset-stats tce [ [ [name] | [glob] | [regex] ] ... ]
```

**Display**

```
list tce
list tce [ [ [name] | [glob] | [regex] ] ... ]
show running-config tce
show running-config tce [ [ [name] | [glob] | [regex] ] ... ]
  options:
    all-properties
    non-default-properties
    one-line
    partition
```

**Delete**

```
delete tce [name]
```
Chapter 33

Description

You can use the tce component to create, modify, display, or delete a TCE profile.

Examples

Creates a custom TCE profile named my_tce_profile:

```
create tce my_tce_profile
```

Displays the properties of the TCE profile:

```
list tce
```

Options

- **description**
  User-defined description.

- **glob**
  Displays the items that match the glob expression. See help glob for a description of glob expression syntax.

- **name**
  Specifies the profile instance name. The name must be tce. This option is required for the modify command.

- **partition**
  Specifies the administrative partition within which the profile resides.

- **regex**
  Specifies the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. See help regex for a description of regular expression syntax.

- **policy**
  Specifies the TCE policy.

See also

edit, glob, list, ltm virtual, modify, regex, reset-stats, show, tmsh, ltm tce-policy
tcp

Configures a Transmission Control Protocol (TCP) profile.

Module

ltm profile

Syntax

Configure the tcp component within the ltm profile module using the following syntax.

Create/Modify

create tcp [ name ]
modify tcp [ name ]

options:
  abc [disabled | enabled]
  ack-on-push [disabled | enabled]
  close-wait-timeout [ integer ]
  cmetrics-cache [disabled | enabled]
  congestion-control [ high-speed | new-reno | none | reno | scalable ]
  defaults-from [ [name] | none ]
  description [string]
  deferred-accept [disabled | enabled]
  delayed-acks [disabled | enabled]
  dsack [disabled | enabled]
  ecn [disabled | enabled]
  fin-wait-timeout [ integer ]
  idle-timeout [ integer ]
  ip-tos-to-client [ integer ]
  keep-alive-interval [ integer ]
  limited-transmit [disabled | enabled]
  link-qos-to-client [ integer ]
  max-retrans [ integer ]
  md5-signature [disabled | enabled]
  md5-signature-passphrase [ none | [string] ]
  nagle [disabled | enabled]
  pkt-loss-ignore-rate [ integer ]
  pkt-loss-ignore-burst [ integer ]
  proxy-buffer-high [ integer ]
  proxy-buffer-low [ integer ]
  proxy-mss [disabled | enabled]
proxy-options [disabled | enabled]
receive-window-size [ integer ]
reset-on-timeout [disabled | enabled]
rfc1323 [disabled | enabled]
selective-acks [disabled | enabled]
send-buffer-size [ integer ]
slow-start [disabled | enabled]
syn-max-retrans [ integer ]
time-wait-recycle [disabled | enabled]
time-wait-timeout [ integer ]
verified-accept [disabled | enabled]
zero-window-timeout [ integer ]
edit tcp [ [ [name] | [glob] | [regex] ] ... ]
options:
   all-properties
   non-default-properties
reset-stats tcp
reset-stats tcp [ [ [name] | [glob] | [regex] ] ... ]

Display

list tcp
list tcp [ [ [name] | [glob] | [regex] ] ... ]
show running-config tcp
show running-config tcp [ [ [name] | [glob] | [regex] ] ... ]
options:
   all-properties
   non-default-properties
   one-line
   partition
show tcp
show tcp [ [ [name] | [glob] | [regex] ] ... ]
options:
   (default | exa | gig | kil | meg | peta | raw | tera | yotta | zetta)
   field-fmt
   global

Delete

delete tcp [name]
Description

You can use the `tcp` component to manage TCP network traffic. Many of the options are standard SYSCTL-types of options, while others are unique to the traffic management system. For most of the options, the default values usually meet your needs. The specific options that you might want to change are: `reset-on-timeout`, `idle-timeout`, `ip-tos-to-client`, and `link-qos-to-client`.

The BIG-IP system installation includes these default TCP-type profiles: `tcp`, `tcp-cell-optimized`, `tcp-lan-optimized`, and `tcp-wan-optimized`. You can modify the values of the options of these profiles or create new TCP-type profiles using any of these existing profiles as parent profiles.

Examples

Creates a custom TCP profile named `my_tcp_profile` that inherits its settings from the system default `tcp` profile:

```
create tcp my_tcp_profile defaults-from tcp
```

Displays all properties for all TCP profiles:

```
list tcp all-properties
```
The options are:

- **high-speed**
  Specifies that the system uses a more aggressive, loss-based algorithm.

- **new-reno**
  Specifies that the system uses a modification to the Reno algorithm that responds to partial acknowledgements when Selective ACKs (SACK) are unavailable.

- **none**
  Specifies that the system does not use a network-congestion-control mechanism, even when congestion occurs.

- **reno**
  Specifies that the system uses an implementation of the TCP Fast Recovery algorithm, which is based on the implementation in the BSD Reno release.

- **scalable**
  Specifies that the system uses a TCP algorithm modification that adds a scalable, delay-based and loss-based component into the Reno algorithm.

- **defaults-from**
  Specifies the profile that you want to use as the parent profile. Your new profile inherits all settings and values from the parent profile. The default value is `tcp`.

- **description**
  User-defined description.

- **deferred-accept**
  Specifies, when enabled, that the system defers allocation of the connection chain context until the client response is received. This option is useful for dealing with 3-way handshake DOS attacks. The default value is `disabled`.

- **delayed-acks**
  Specifies, when enabled, the default value, that the traffic management system allows coalescing of multiple acknowledgement (ACK) responses.

- **dsack**
  When enabled, specifies the use of the `selective-acks` option to acknowledge duplicate segments. The default value is `disabled`.

- **ecn**
  Specifies, when enabled, that the system uses the TCP flags `CWR` and `ECE` to notify its peer of congestion and congestion counter-measures. The default value is `disabled`.

- **fin-wait-timeout**
  Specifies the number of seconds that a connection is in the FIN-WAIT or closing state before quitting. The default value is 5 seconds. A value of 0 (zero) represents a term of forever (or until the matrix of the FIN state).
- **glob**
  Displays the items that match the `glob` expression. For a description of `glob` expression syntax, see the `glob` man page.

- **idle-timeout**
  Specifies the number of seconds that a connection is idle before the connection is eligible for deletion. The default value is 300 seconds.

- **ip-tos-to-client**
  Specifies the Type of Service (ToS) level that the traffic management system assigns to TCP packets when sending them to clients. The default value is 0 (zero).

- **keep-alive-interval**
  Specifies the keep-alive probe interval, in seconds. The default value is 1800 seconds.

- **limited-transmit**
  Specifies, when enabled, the default value, that the system uses limited transmit recovery revisions for fast retransmits (as specified in RFC 3042) to reduce the recovery time for connections on a lossy network.

- **link-qos-to-client**
  Specifies the Link Quality of Service (QoS) level that the system assigns to TCP packets when sending them to clients. The default value is 0 (zero).

- **max-retrans**
  Specifies the maximum number of retransmissions of data segments that the system allows. The default value is 8.

- **md5-signature**
  Specifies, when enabled, that the system uses RFC2385 TCP-MD5 signatures to protect TCP traffic against intermediate tampering. The default value is disabled.

- **md5-signature-passphrase**
  Specifies a plain text passphrase which can be between 1 and 80 characters in length, and is used in a shared-secret scheme to implement the spoof-prevention parts of RFC2385. The default value is none.

- **nagle**
  Specifies, when enabled, that the system applies Nagle's algorithm to reduce the number of short segments on the network. For interactive protocols such as Telnet, rlogin, or SSH, F5 Networks recommends disabling this option on high-latency networks, to improve application responsiveness. The default value is disabled.

- **name**
  Specifies a unique name for the component. This option is required for the commands create, delete, and modify.

- **partition**
  Displays the administrative partition within which the component resides.
◆ **pkt-loss-ignore-rate**
   Specifies the threshold of packets lost per million at which the system performs congestion control. Valid values are 0 (zero) through 1,000,000. The default value is 0 (zero), which means that the system performs congestion control if any packet loss occurs. If you set the ignore rate to 10 and packet loss for a TCP connection is greater than 10 per million, congestion control occurs.

◆ **pkt-loss-ignore-burst**
   Specifies the probability of performing congestion control when multiple packets in a row are lost, even if the *pkt-loss-ignore-rate* was not exceeded. Valid values are 0 (zero) to 32. The default value is 0 (zero), which means that the system performs congestion control, if any packets are lost. Higher values decrease the chance of performing congestion control.

◆ **proxy-buffer-high**
   Specifies the highest level at which the receive window is closed. The default value is 49152.

◆ **proxy-buffer-low**
   Specifies the lowest level at which the receive window is closed. The default value is 32768.

◆ **proxy-mss**
   Specifies, when enabled, that the system advertises the same mss to the server as was negotiated with the client. The default value is disabled.

◆ **proxy-options**
   Specifies, when enabled, that the system advertises an option, such as a timestamp to the server only if it was negotiated with the client. The default value is disabled.

◆ **receive-window-size**
   Specifies the size of the receive window, in bytes. The default value is 65535 bytes.

◆ **regex**
   Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. For a description of regular expression syntax, see the regex man page.

◆ **reset-on-timeout**
   Specifies whether to reset connections on timeout. The default value is enabled.

◆ **rfc1323**
   Specifies, when enabled, the default value, that the system uses the timestamp and window-scaling extensions for TCP (as specified in RFC 1323) to enhance high-speed network performance.

◆ **selective-acks**
   Specifies, when enabled, the default value, that the system negotiates RFC2018-compliant Selective Acknowledgements with peers.

◆ **send-buffer-size**
   Specifies the size of the buffer, in bytes. The default value is 65535.
- **slow-start**
  Specifies, when enabled, the default value, that the system uses larger initial window sizes (as specified in RFC 3390) to help reduce round trip times. Note that disabling this attribute causes the setting for `cmetrics-cache` to be ignored.

- **syn-max-retrans**
  Specifies the maximum number of retransmissions of SYN segments that the system allows. The default value is 3.

- **time-wait-recycle**
  Specifies whether the system recycles the connection when a SYN packet is received in a TIME-WAIT state. The default value is enabled.

- **time-wait-timeout**
  Specifies the number of seconds that a connection is in the TIME-WAIT state before closing. The default value is 2000 seconds.

- **verified-accept**
  Specifies, when enabled, that a SYN-ACK acknowledgement code is sent only if the server port is open. The default value is disabled.

- **zero-window-timeout**
  Specifies the timeout in milliseconds for terminating a connection with an effective zero length TCP transmit window. The timeout starts when the peer advertises a zero length TCP window or when enough data has been sent to fill the previously advertised window. The timer is canceled when a non-zero length window is received. The default value is 20000 milliseconds.

### See also

create, delete, edit, glob, list, ltm virtual, modify, regex, reset-stats, show, tmsh
udp

Configures a User Datagram Protocol (UDP) profile.

Module

ltm profile

Syntax

Configure the udp component within the ltm profile module using the following syntax.

Create/Modify

create udp [name]
modify udp [name]
  options:
    allow-no-payload [disabled | enabled]
    datagram-load-balancing [disabled | enabled]
    defaults-from [ [name] | none]
    description [string]
    idle-timeout [immediate | indefinite | integer]
    ip-tos-to-client [ [integer] | pass-through]
    link-qos-to-client [ [integer] | pass-through]
    no-checksum [disabled | enabled]
edit udp [ [ [name] | [glob] | [regex] ] ... ]
  options:
    all-properties
    non-default-properties
reset-stats udp
reset-stats udp [ [ [name] | [glob] | [regex] ] ... ]

Display

list udp
list udp [ [ [name] | [glob] | [regex] ] ... ]
show running-config udp
show running-config udp [ [ [name] | [glob] | [regex] ] ... ]
  options:
    all-properties
    non-default-properties
    one-line
    partition
show udp
show udp [ [ [name] | [glob] | [regex] ] ... ]

options:
  (default | exa | gig | kil | meg | raw | peta | tera | yotta | zetta)
field-fmt
  global

Delete

delete udp [name]

Description

You can use the udp component to manage UDP network traffic.

Examples

Creates a custom UDP profile named my_udp_profile that inherits its settings from the system default UDP profile:
create udp my_udp_profile defaults-from udp

Displays all properties for all UDP profiles:
list udp all-properties

Options

You can use these options with the udp component:

- **allow-no-payload**
  Provides the ability for the passage of datagrams that contain header information, but no essential data. The default value is disabled.

- **datagram-load-balancing**
  Provides the ability to load balance UDP datagram by datagram. The default value is disabled.

- **defaults-from**
  Specifies the profile that you want to use as the parent profile. Your new profile inherits all settings and values from the parent profile. The default value is udp.

- **description**
  User-defined description.

- **glob**
  Displays the items that match the glob expression. For a description of glob expression syntax, see the glob man page.

- **idle-timeout**
  Specifies the number of seconds that a connection is idle before the connection is eligible for deletion. The default value is 60 seconds.
◆ **ip-tos-to-client**  
Specifies the Type of Service (ToS) level that the traffic management system assigns to UDP packets when sending them to clients. The default value is \(0\) (zero).

◆ **link-qos-to-client**  
Specifies the Link Quality of Service (QoS) level that the system assigns to UDP packets when sending them to clients. The default value is \(0\) (zero).

◆ **name**  
Specifies a unique name for the component. This option is required for the commands `create`, `delete`, and `modify`.

◆ **no-checksum**  
Enables or disables checksum processing. The default value is `disabled`. If the datagram is IPv6, the system always performs checksum processing.

◆ **partition**  
Displays the administrative partition within which the component resides.

◆ **regex**  
Displays the items that match the regular expression. The regular expression must be preceded by an at sign (`@[regular expression]`) to indicate that the identifier is a regular expression. For a description of regular expression syntax, see the `regex` man page.

**See also**

`create`, `delete`, `edit`, `glob`, `list`, `ltm profile`, `ltm virtual`, `modify`, `regex`, `reset-stats`, `show`, `tmsh`
wa-cache

Manages the BIG-IP system WebAccelerator™ cache.

Module

ltm profile

Syntax

Configure the wa-cache component within the ltm profile module using the syntax shown in the following sections.

Display

show wa-cache
show wa-cache [ [ [name] | [glob] | [regex] ] ... ]

options:
  exact
  host [string]
  max-response [integer]
  uri [string]

Delete

delete wa-cache [name]

Description

You can use the wa-cache component to delete the entries in or show information about the BIG-IP system WebAccelerator cache.

Examples

Displays information about the entries in the BIG-IP system cache:

show wa-cache

Deletes the entries in the BIG-IP system WebAccelerator cache:

delete wa-cache
Options

You can use these options with the `wa-cache` component:

- **exact**
  Displays the exact number of entries in the WebAccelerator cache.

- **host**
  Displays the host from which the entry was cached.

- **max-response**
  Displays the maximum number of entries that can be in the WebAccelerator cache. The default value is 0 (zero), which means that the system does not limit the maximum entries.

- **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an `@` sign (`@[regular expression]`) to indicate that the identifier is a regular expression. See `help regex` for a description of regular expression syntax.

- **uri**
  Displays the URI from which the entry was cached.

See also

`delete`, `show`, `tmsh`
xml

Configures an XML profile.

Module

ltm profile

Syntax

Configure the xml component within the ltm profile module using the following syntax.

Create/Modify

create xml [name]
modify xml [name]

options:
  defaults-from [ [name] | none]
  description [string]
  namespace-mappings [ [none] |
   { mapping-namespace amepace1 mapping-prefix prefix1 }
  xpath-queries [ none | [ add | delete | replace_all_with { queries } ] ]

edit xml [ [ [name] | [glob] | [regex] ] ... ]

options:
  all-properties
  non-default-properties

Display

list xml
list xml [ [ [name] | [glob] | [regex] ] ... ]
show running-config xml
show running-config xml [ [ [name] | [glob] | [regex] ] ... ]

options:
  all-properties
  non-default-properties
  one-line
  partition

Delete

delete xml [name]
Chapter 33

Description

Use this command to create, modify, display, or delete an XML profile with which you can use XML functionality.

Examples

Creates a custom XML profile named `my_xml_profile` that inherits its settings from the system default XML profile:

```bash
create xml my_xml_profile defaults-from xml
```

Displays the properties of all XML profiles:

```bash
list xml
```

Options

You can use these options with the `xml` component:

- **defaults-from**
  - Specifies the profile that you want to use as the parent profile. Your new profile inherits all settings and values from the parent profile specified. The default value is `xml`.

- **description**
  - User-defined description.

- **glob**
  - Displays the items that match the `glob` expression. See `help glob` for a description of `glob` expression syntax.

- **name**
  - Specifies a unique name for the component. This option is required for the `create`, `delete`, and `modify` commands.

- **partition**
  - Displays the administrative partition within which the component resides.

- **namespace-mappings**
  - Specifies a list of mappings between namespaces and prefixes to be used in the XPath queries of the profile.

- **regex**
  - Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. For a description of regular expression syntax, see the `regex` man page.

- **xpath-queries**
  - Specifies the list of XPath queries that are used by the profile. A match of any of the queries triggers the XML_CONTENT_BASED_ROUTING iRule event.
See also

create, delete, edit, glob, list, ltm virtual, modify, regex, reset-stats, show, tmsh
Introducing the ltm tce module

Alphabetical list of components
Introducing the ltm tce module

You can use the \texttt{tmsh} components that reside within the \texttt{ltm tce} module to configure Local Traffic Manager™. For more information about the \texttt{tmsh} hierarchical structure, see Chapter 2, \textit{Understanding and Using the Traffic Management Shell}.

Alphabetical list of components

The remainder of this chapter lists the \texttt{tmsh} components that are available in the \texttt{ltm tce} module.
**policy**

Configures Traffic Control and Enforcement (TCE) policies for the Policy Enforcement Manager (PEM).

**Module**

**ltm tce**

**Syntax**

Configure the **policy** component within the **ltm tce** module using the syntax shown in the following sections.

**Create/Modify**

```plaintext
create policy [name]
modify policy [name]
    options:
        description [string]
        rule [add | delete | modify | none | replace-all-with] {
            [ [rule_name] ] {
                options:
                    category [category_name]
                    description [string]
                    protocol [protocol_name]
                    steering [steering_name]
            }
        }
edit policy [ [ [name] | [glob] | [regex] ] ... ]
    options:
        all-properties
        non-default-properties
```

**Display**

```plaintext
list policy
list policy [ [ [name] | [glob] | [regex] ] ... ]
show running-config policy
show running-config policy [ [ [name] | [glob] | [regex] ] ... ]
options:
    all-properties
    non-default-properties
    one-line
    partition
```
Delete

delete policy [name]

◆ Note
You must remove all references to a policy before you can delete the policy.

Description

You can use the **policy** component to configure the TCE policy definitions on the Policy Enforcement Manager.

Examples

Creates a Policy Enforcement Manager policy named **my_policy** with two TCE rules: **my_rule_1** and **my_rule_2**. The **my_rule_1** policy defines the matching (category, protocol) to be (P2P, bittorrent) and the steering action defined by **my_endpoint_1**. The **my_rule_2** policy defines the matching (category, protocol) to be (web, all) and the steering action defined by **my_endpoint_2**.

```bash
create policy my_policy rule add {
    my_rule_1 {
        category audio
        protocol http
        steering my_endpoint_1
    }
    my_rule_2 {
        category web
        protocol http
        steering my_endpoint_2
    }
}
```

Deletes the policy named **my_policy**:

delete policy my_policy

Displays the properties of the policy named **my_policy**:

```bash
list policy my_policy
```

Options

You can use these options with the **policy** component:

◆ **category**
  
  Specifies the matching category.
◆ **description**  
User-defined description.

◆ **protocol**  
Specifies the matching protocol.

◆ **steering**  
Specifies the steering endpoint.

**See Also**

create, delete, edit, glob, list, modify, ltm tce steering-endpoint, regex, reset-stats, show, tmsh
steering-endpoint

Configures steering endpoints for the Policy Enforcement Manager (PEM).

Module

ltm tce

Syntax

Configure the steering-endpoint component within the ltm tce module using the syntax shown in the following sections.

Create/Modify

create steering-endpoint [name]
modify steering-endpoint [name]

options:
  description [string]
pool [pool_name]
  snatpool [snatpool_name]
  source-port [change | preserve | preserve-strict]
  translate-address [enabled | disabled]
  translate-port [enabled | disabled]
edit steering-endpoint [ [name] | [glob] | [regex] ] ... ]

options:
  all-properties
  non-default-properties

Display

list steering-endpoint
list steering-endpoint [ [name] | [glob] | [regex] ] ... ]
show running-config steering-endpoint
show running-config steering-endpoint [ [name] | [glob] | [regex] ] ... ]

options:
  all-properties
  non-default-properties
  one-line
  partition
Delete

```
delete steering-endpoint [name]
```

◆ Note

You must remove all references to a steering endpoint before you can delete the steering endpoint.

Description

You can use the `steering-endpoint` component to configure steering endpoint definitions for the Policy Enforcement Manager.

Examples

Creates a Policy Enforcement Manager steering endpoint named `my_endpoint`:

```
create steering-endpoint my_endpoint { pool my_pool snatpool my_snatpool source-port preserved translate-address enabled translate-port enabled }
```

Deletes the steering endpoint named `my_endpoint`:

```
delete steering-endpoint my_endpoint
```

Displays the properties of the steering endpoint named `my_endpoint`:

```
list steering-endpoint my_endpoint
```

Options

◆ **description**
User-defined description.

◆ **pool**
Specifies the name of an existing pool to which you want the steering endpoint to automatically direct traffic. You must specify a valid pool name.

◆ **snatpool**
Specifies the name of an existing SNAT pool that you want the steering endpoint to use to implement selective and intelligent SNATs. The default value is `none`.

◆ **translate-address**
Enables or disables address translation for the steering endpoint. Disable address translation for a steering endpoint if you want to use the steering endpoint to direct traffic to any address. The default value is `disabled`.

◆ **translate-port**
Enables or disables port translation for the steering endpoint. Disable port translation for a steering endpoint if you want to use the steering endpoint to direct the traffic to any port. The default value is `disabled`.
See Also

create, delete, edit, glob, list, modify, ltm tce policy, regex, reset-stats, show, tmsh
net Module Components

- Introducing the net module
- Alphabetical list of components
Introducing the net module

You can use the `tmsh` components that reside within the `net` module to configure the network. For more information about the `tmsh` hierarchical structure, see Chapter 2, *Understanding and Using the Traffic Management Shell*.

Alphabetical list of components

The remainder of this chapter lists the `tmsh` components that are available in the `net` module.
arp

Manages entries in the Address Resolution Protocol (ARP) table.

Module

net

Syntax

Configure the arp component within the net module using the following syntax.

Create/Modify

create arp [name]
modify arp [name]
  options:
    mac-address [mac address]
edit arp [ [ [name] | [glob] | [regex] ] ... ]
  options:
    all-properties
    non-default-properties

Display

list arp
list arp [ [ [name] | [glob] | [regex] ] ... ]
show running-config arp
show running-config arp [ [ [ip address] | [glob] | [regex] ] ... ]
  options:
    all-properties
    non-default-properties
show arp
show arp [ [ [name] | [glob] | [regex] ] ... ]
  options:
    [dynamic | static ]

Delete

delete arp [name]
Description

You can use the `arp` component to add entries to or delete entries from the ARP table.

You can create static ARP entries for IPv4 addresses to link-layer addresses, such as Ethernet media access control (MAC) addresses. You can view and delete static and dynamic ARP entries.

You can also use the `db` component in the `sys` module to configure how the system handles ARP entries for dynamic timeout, maximum dynamic entries, add reciprocal, and maximum retries. For more information, see `db`, on page 39-24.

Examples

- Creates an ARP mapping of the IP address `10.10.10.20` to the MAC address `00:0b:09:88:00:9a`, and the name of this entry is `myARP`. Alternatively, the address can be used as the name, like the next example:

  ```
  create arp myARP ip-address 10.10.10.20 mac-address 00:0b:09:88:00:9a
  ```

- Creates an ARP mapping of IP address `10.10.10.20` to the MAC address `00:0b:09:88:00:9a`:

  ```
  create arp 10.10.10.20 mac-address 00:0b:09::88:00:9a
  ```

- Modifies the ARP mapping of the ARP entry named `10.10.10.20` to the MAC address `00:0b:09:88:00:9b`:

  ```
  modify arp 10.10.10.20 mac-address 00:0b:09:88:00:9b
  ```

- Displays ARP status and statistics for the system:

  ```
  show arp
  ```

- Displays ARP status and statistics for all IP addresses in route domain 2. A `glob` expression displays the same result:<

  ```
  show arp *%2
  ```

- Displays all properties for all ARP entries for the system:

  ```
  list arp all-properties
  ```

- Displays all non-default properties for all ARP entries for the system:

  ```
  list arp non-default-properties
  ```

- Deletes all ARP entries for the system:

  ```
  delete arp all
  ```

- Deletes the ARP entry named `myARP`:

  ```
  delete arp myARP
  ```
Options

You can use these options with the `arp` component:

- **description**
  User-defined description.

- **dynamic**
  Displays the status of dynamic ARP entries.

- **glob**
  Displays the items that match the `glob` expression. For a description of `glob` expression syntax, see the `glob` man page.

- **ip address**
  The IP address to be mapped. This is optional, and if not present, the name needs to be a string that represents a valid IP address.

- **mac-address**
  Specifies a 6-byte ethernet address in not case-sensitive hexadecimal colon notation, for example: `00:0b:09:88:00:9a`. You must specify a MAC address when you create an ARP entry.

- **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. For a description of regular expression syntax, see the `regex` man page.

- **static**
  Displays the status of static ARP entries.

See also

create, delete, edit, glob, list, modify, regex, show, tmsh
cmetrics

Displays and deletes entries in the route metrics table on the BIG-IP® system.

Module

net

Syntax

Configure the cmetrics component within the net module using the following syntax.

Display

show cmetrics
option:
  bandwidth
dest-addr [ip address]
hwaddress
mtu
rtt
rttvar
ssthresh
tmm

Delete

delete cmetrics
option:
dest-addr [IP address]

Description

You can use the cmetrics component to display entries in the route metrics table on the BIG-IP system. Additionally, you can delete a specified route metric entry from the table. The options are display-only values and cannot be used for filtering.

◆ Note

You can delete only entries that have no connection references.
Examples

Displays all the entries in the route metrics table:

```
show cmetrics
```

Deletes the entry with destination IP address 10.10.1.11 from the route metrics table:

```
delete cmetrics dest-addr 10.10.1.11
```

Options

You can use these options with the `arp` component:

- `bandwidth`
  Displays the size of the channel.

- `dest-addr`
  Specifies the destination IP address of the entry that you want to display or delete. You can enter this address in either IPv4 or IPv6 format.

- `hwaddress`
  Displays the Media Access Control (MAC) address for the route.

- `mtu`
  Displays the maximum transmit unit size on the route.

- `rtt`
  Displays the round-trip time on the route.

- `rttvar`
  Displays the variance in the round-trip time.

- `ssthresh`
  Displays the cached slow-start threshold.

- `tmm`
  Displays the identifying number of the TMM (Traffic Management Microkernel).

See also

```
delete, show, tmsh
```
**fdb**

Manages entries in the Layer 2 Forwarding table.

**Module**

net

**Syntax**

Configure the **fdb** component within the **net** module using the following syntax.

**Modify**

```bash
modify fdb [vlan name]
```

```bash
options:
  records
    [add | delete | modify | replace-all-with] {
      [MAC address] ... {
        description [string]
        trunk [trunk name]
        interface [interface name]
      }
    }
  records none
```

```bash
edit fdb [ [ all | [ vlan name] | [glob] | [regex] ] ...]
```

```bash
options:
  all-properties
  non-default-properties
```

**Display**

```bash
list fdb
```

```bash
list fdb [ [ vlan name] | [glob] | [regex] ] ...
```

```bash
show running-config fdb
```

```bash
show running-config fdb [ [ vlan name] | [glob] | [regex] ] ...
```

```bash
options:
  all-properties
  non-default-properties
  one-line
  partition
  records
```
Chapter 35

show fdb
show fdb [ [ [ vlan name ] | [glob] | [regex] ] ...]
   options:
      dynamic
      field-fmt
      static

Delete

delete fdb
delete fdb [all | [vlan name] ]
   options:
      all-records
      dynamic
      static

Description

You can use the fdb component to manage entries in the VLAN Layer 2 Forwarding table.

Examples

Creates a mapping of the MAC address 00:0b:09:88:00:9a to interface 1.2 on VLAN internal.
modify fdb internal records add { 00:0b:09:88:00:9a { 
      interface 1.2 } }

Modifies the mapping of the MAC address 00:0b:09:88:00:9b to interface 1.1 on VLAN internal.
modify fdb internal records modify { 00:0b:09:88:00:9a { 
      interface 1.1 } }

Displays all dynamic and static entries in the Layer 2 Forwarding table:
show fdb

Displays all properties for all static entries in the Layer 2 Forwarding table:
list fdb all-properties

Displays all non-default properties for all static entries in the Layer 2 Forwarding table:
list fdb non-default-properties

Deletes all entries in the VLAN Layer 2 Forwarding tables:
delete fdb all
Options

You can use these options with the fdb component:

- **all-records**
  Deletes, from the specified VLAN, all dynamic and static records.

- **description**
  User-defined description.

- **dynamic**
  Displays or deletes all dynamic entries in the Layer 2 Forwarding table.

- **glob**
  Displays the items that match the glob expression. For a description of glob expression syntax, see the glob man page.

- **interface**
  Specifies an interface to which you want to map a MAC address. You must specify either an interface or a trunk when you create an entry in the Layer 2 Forwarding table.

- **mac-address**
  Specifies a 6-byte ethernet address in not case-sensitive hexadecimal colon notation, for example: **00:0b:09:88:00:9a**. You must specify a MAC address when you create an entry in the Layer 2 Forwarding table.

- **partition**
  Displays the administrative partition in which the VLAN resides.

- **records**
  Specifies MAC addresses that you want to add to, delete from, modify, or replace in the VLAN Layer 2 Forwarding table.

- **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. For a description of regular expression syntax, see the regex man page.

- **static**
  Displays or deletes all static entries in the Layer 2 Forwarding table.

- **trunk**
  Specifies a trunk to which you want to map a MAC address. You must specify either an interface or a trunk when you create an entry in the Layer 2 Forwarding table.

See also

delete, edit, glob, list, modify, net vlan, regex, show, tmsh
interface

Configures the parameters of interfaces.

Module

net

Syntax

Configure the interface component within the net module using the syntax in the following sections.

Modify

modify interface [name]

options:
  description [string]
  [disabled | enabled]
  flow-control (none | rx | tx | tx-rx)
  force-gigabit-fiber [enabled | disabled]
  media [auto | 10baseT half | 10baseT full | 100baseT half |
         100baseT full | 1000baseT half | 1000baseT full |
         1000baseSX full | 1000baseLX full | 1000baseCX full |
         10GbaseT full | 10GbaseSR full | 10GbaseLR full |
         10GbaseER full | 10SFP+Cu full | 40GbaseSR4 full |
         40GbaseLR4 full | none | no-phy]
  media-fixed [auto | 10baseT half | 10baseT full |
              100baseT half | 100baseT full | 1000baseT half |
              1000baseT full | none | no-phy]
  media-sfp [auto | 10baseT half | 10baseT full | 100baseT half |
             100baseT full | 1000baseT half | 1000baseT full |
             1000baseSX full | 1000baseLX full | 1000baseCX full |
             10GbaseT full | 10GbaseSR full | 10GbaseLR full |
             10GbaseER full | 10SFP+Cu full | 40GbaseSR4 full |
             40GbaseLR4 full | none | no-phy]
  prefer-port [fixed | sfp]
  stp [disabled | enabled]
  stp-auto-edge-port [enabled | disabled]
  stp-edge-port [false | true]
  stp-link-type [auto | p2p | shared]
  stp-reset

edit interface [ [ [name] | [glob] | [regex] ] ... ]

options:
  all-properties
  non-default-properties

reset-stats interface

reset-stats interface [ [ [name] | [glob] | [regex] ] ... ]

Display

list interface

list interface [ [ [name] | [glob] | [regex] ] ... ]

show running-config interface
show running-config interface
   [ [ [name] | [glob] | [regex] ] ... ]
   options:
      all-properties
      mac-address
      media-active
      media-capabilities
      media-max
      mtu
      non-default-properties
      (pending | not-pending)
      one-line

show interface
   show interface [ [ [name] | [glob] | [regex] ] ... ]
   options:
      all-properties
      (default | exa | gig | kil | meg | peta | raw | tera | yotta | zetta)
      field-fmt

Description

You can use the `interface` component to enable or disable an interface, and to display and set media options, duplex mode, and status for an interface. In addition, you can specify whether the interface participates in the spanning tree protocol (STP) configuration, and set per-interface STP parameters such as link type, edge port status, and automatic edge port detection.

Examples

modify interface 1.1 enabled
Enables the interface named 1.1.
modify interface 1.2 disabled
Disables the interface named 1.2.
modify interface 1.1 1.2 1.3 stp disable
Disables STP on the interfaces named 1.1, 1.2, and 1.3.
modify interface 1.1 1.2 1.3 stp-auto-edge-port enabled
Sets auto edge detection for STP on the interfaces named 1.1, 1.2, and 1.3.
modify interface 1.1 1.2 1.3 stp-edge-port true
Sets the edge port attribute for STP on the interfaces named 1.1, 1.2, and 1.3.

Options

- description
  User defined description.
- [disabled | enabled]
  Enables or disables the specified interface. The default value is enabled.
◆ **flow-control**
   Specifies how the system controls the sending of PAUSE frames for flow control. The default value is **tx-rx**.
   - **none**
     Disables flow control.
   - **rx**
     Specifies that the interface honors pause frames from its partner, but does not generate pause frames.
   - **tx**
     Specifies that the interface ignores pause frames from its partner, and generates pause frames when necessary.
   - **tx-rx**
     Specifies that the interface honors pause frames from its partner, and also generates pause frames when necessary.

◆ **force-gigabit-fiber**
   Enables or disables forcing of gigabit fiber media. If this is enabled for a gigabit fiber interface, the media setting will be forced, and no auto-negotiation will be performed. If it is disabled, auto-negotiation will be performed with just a single gigabit fiber option advertised.

◆ **glob**
   Displays the items that match the **glob** expression. See **help glob** for a description of **glob** expression syntax.

◆ **interface-index**
   Displays the interface index assigned to this interface. It is a unique identifier assigned for all objects displayed in the SNMP IF-MIB.

◆ **mac-address**
   Displays the 6-byte ethernet address in not case-sensitive hexadecimal colon notation, for example, **00:0b:09:88:00:9a**.

◆ **media**
   Specifies the settings for the interface. The possible values are: 10baseT-full, 10baseT-half, 10GbaseER-full, 10GbaseLR-full, 10GbaseSR-full, 10GbaseT-full, 10GbaseSR+full, 40GbaseLR4-full, 40GbaseLR4-half, 100baseTX-half, 100baseTX-full, 100baseLX-full, 1000baseCX-full, 1000baseT-full, 1000baseT-half, 1000baseSX-full, auto, none, and no-phy.
   When you set the **media** option, the system automatically sets either the **media-sfp** or **media-fixed** option, based on whether the interface supports small factor form pluggable (SFP) interfaces, or for combo ports whether SFP is the preferred port.

◆ **media-active**
   Displays the current media setting for the interface.

◆ **media-fixed**
   Specifies the settings for a fixed (non-pluggable) interface. Use this option only with a combo port to specify the media type for the fixed interface, when it is not the preferred port.

◆ **media-max**
   Displays the maximum media value for the interface.
◆ **media-sfp**
Specifies the settings for an SFP (pluggable) interface. Note that you use this option only with a combo port to specify the media type for the SFP interface, when it is not the preferred port.

◆ **mtu**
Displays the Maximum Transmission Unit (MTU) of the interface, which is the maximum number of bytes in a frame without IP fragmentation.

◆ **name**
Specifies an interface name, for example `3.1`, where 3 is the physical slot number holding the network interface hardware and 1 is the physical port number of that interface on that hardware. Another example is `mgmt`, the name given to the management interface.

◆ `[pending | not-pending]`
*Pending* indicates that the slot with which the interface is associated does not contain a blade. *Not-pending* indicates that the slot with which the interface is associated is not a cluster member. The default value is `pending`.

◆ **prefer-port**
Indicates which side of a combo port the interface uses, if both sides of the port have the potential for external links. The default value is `sfp`. Do not use this option for non-combo ports.

◆ **regex**
Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. See `help regex` for a description of regular expression syntax.

◆ **serial**
Displays the serial number of the pluggable unit on an interface. It is only available on a SFP/SFP+/XFP/QSFP+ unit.

◆ **stp**
Enables or disables STP. If you disable STP, no STP, RSTP, or MSTP packets are transmitted or received on the interface or trunk, and spanning tree has no control over forwarding or learning on the port or the trunk. The default value is `enabled`.

◆ **stp-auto-edge-port**
Sets the STP automatic edge port detection for the interface. The default value is `enabled`. When STP automatic edge port detection is set to `enabled` on an interface, the system monitors the interface for incoming STP, RSTP, or MSTP packets. If no such packets are received for a sufficient period of time (about three seconds), the interface is automatically given edge port status. When automatic edge port detection is set to `disabled` on an interface, the system does not automatically give the interface the edge port status. Any STP setting set on a per-interface basis applies to all spanning tree instances.

◆ **stp-edge-port**
Sets STP edge port detection. The default value is `true`. 
◆ stp-link-type
Specifications the STP link type for the interface. The default value is auto. The spanning tree system includes important optimizations that can only be used on point-to-point links. That is, on links that connect just two bridges. If these optimizations are used on shared links, incorrect or unstable behavior may result. By default, the implementation assumes that full-duplex links are point-to-point and that half-duplex links are shared.
The options are:
• auto
  Specifies that the system determines the spanning tree link type, which is based on the duplex setting.
• p2p
  Specifies that the system uses the optimizations for point-to-point spanning tree links. Point-to-point links connect only two spanning tree bridges.
• shared
  Specifies that the system uses the optimizations for shared spanning tree links. Shared links connect two or more spanning tree bridges.
◆ stp-reset
Resets STP, which forces a migration check.
◆ vendor
Displays the name of the vendor of the pluggable unit on an interface. It is only available on a SFP/SFP+/XFP/QSFP+ unit.

See Also

edit, glob, list, modify, regex, reset-stats, show, tmsh
ndp

Configures IPv6-to-Ethernet neighbor discovery display and control.

Module

net

Syntax

Configure the ndp component within the net module using the following syntax.

Create/Modify

create ndp [name]
modify ndp [name]
  options:
    mac-address [MAC address]
edit ndp [ [name] | [glob] | [regex] ] ...
  options:
    all-properties
    non-default-properties

Display

list ndp
list ndp [ [name] | [glob] | [regex] ] ...
show running-config ndp
show running-config ndp [ [name] | [glob] | [regex] ] ...
  options:
    all-properties
    non-default-properties
    one-line
show ndp
show ndp [ [name] | [glob] | [regex] ] ...
  options:
    [dynamic | static]

Delete

dele ndp [name]
Description

Configures the IPv6-to-Ethernet address translation tables used by the IPv6 neighbor discovery protocol.

Examples

Maps the IPv6 address, \texttt{fec0:f515::c001}, to the MAC address, \texttt{00:0B:DB:3F:F6:57}, and the name of this entry is \texttt{myNdp}. Alternatively, the address can be used as the name, like the following example:

\begin{verbatim}
create ndp myNdp ip-address fec0:f515::c001 mac-address 00:0B:DB:3F:F6:57
\end{verbatim}

Maps the IPv6 address, \texttt{fec0:f515::c001}, to the MAC address, \texttt{00:0B:DB:3F:F6:57}:

\begin{verbatim}
create ndp fec0:f515::c001 mac-address 00:0B:DB:3F:F6:57
\end{verbatim}

Displays static and dynamic IPv6 address-to-MAC address mapping:

\texttt{show ndp}

Options

You can use the following options with the \texttt{ndp} component:

\begin{itemize}
  \item \texttt{dynamic}
    Displays dynamic IPv6 address-to-MAC address mapping.
  \item \texttt{glob}
    Displays the items that match the \texttt{glob} expression. For a description of \texttt{glob} expression syntax, see the \texttt{glob} man page.
  \item \texttt{ip-address}
    The IP address that is to be mapped. This is optional, and if not present, the name needs to be a string that represents a valid IP address.
  \item \texttt{mac-address}
    Specifies a 6-byte Ethernet address in hexadecimal colon notation that is not case-sensitive. For example, \texttt{00:0B:09:88:00:9a}.
  \item \texttt{regex}
    Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. For a description of regular expression syntax, see the \texttt{regex} man page.
  \item \texttt{static}
    Displays static IPv6 address-to-MAC address mapping.
\end{itemize}

See also

\texttt{create, delete, edit, glob, list, modify, regex, show, tmsh}
packet-filter

Configures packet filter rules.

Module

net

Syntax

Configure the packet-filter component within the net module using the following syntax.

Create/Modify

create packet-filter [name]
modify packet-filter [name]

options:
  action [accept | continue | discard | reject]
  description [string]
  logging [enabled | disabled]
  order [integer]
  rate-class [name]
  rule "[BPF expression]"
  vlan [name]

edit packet-filter [ [ [name] | [glob] | [regex] ] ... ]

options:
  all-properties
  non-default-properties

reset-stats packet-filter
reset-stats packet-filter [ [ [name] | [glob] | [regex] ] ... ]

Display

list packet-filter
list packet-filter [ [ [name] | [glob] | [regex] ] ... ]

show running-config packet-filter
show running-config packet-filter [ [ [name] | [glob] | [regex] ] ... ]

options:
  all-properties
  non-default-properties
  one-line
You can use the `packet-filter` component to create a layer of security for the traffic management system using packet filter rules.

The BIG-IP system packet filters are based on the Berkeley Software Design Packet Filter (BPF) architecture. Packet filter rules are composed of four mandatory attributes and three optional attributes. The mandatory attributes are `name`, `order`, `action`, and `rule`. The optional attributes are `vlan`, `logging`, and `rate-class`. The rule attribute you choose defines the BPF script to match for the rule.

**Important**

*By default, packet filtering is disabled. You must enable packet filtering using the Configuration utility. For more information, see the BIG-IP® Traffic Management Operating System®: Implementations.*

### Examples

You can create a set of rules that specify what incoming traffic you want the system to accept and how to accept it. See the following examples.

#### Example 1: Block spoofed addresses

This example prevents private IP addresses from being accepted on a public VLAN. This is a way of ensuring that no one can spoof private IP addresses through the external VLAN of the system. In this example, the system logs when this happens:

```plaintext
create packet-filter spoof_blocker {
    order 5
    action discard
    vlan external
    logging enabled
    rule { ( src net 172.19.255.0/24 )}
}
```
Example 2: Allow restricted management access

You can provide restricted SSH and HTTPS access to the traffic management system for management purposes and keep a log of that access. However, this is not the same management access you can get through the management port/interface (`mgmt`); that interface is not affected by any packet filter configuration and if that is the only way you want to provide access to your system, this configuration is not necessary.

In the first rule, following, SSH is allowed access from a single fixed-address administrative workstation, and each access is logged. In the subsequent rule, browser-based Configuration utility access is allowed from two fixed-address administrative workstations; however, access is not logged.

```plaintext
create packet-filter management_ssh {
  order 10
  action accept
  logging enabled
  rule { ( proto TCP ) and ( src host 172.19.254.10 ) and ( dst port 22 )}
}
create packet-filter management_gui {
  order 15
  action accept
  rule { ( proto TCP ) and ( src host 172.19.254.2 or src host 172.19.254.10 ) and \ 
    ( dst port 443))
}
```

Example 3: Allow access to all virtual servers

In this final example, you can verify that all of the virtual servers in your configuration are reachable from the public network. This is critical if you have decided to use a default-deny policy. A `default-deny policy` restricts Internet access to everything that is not explicitly permitted. This example also shows how to rate shape all traffic to the virtual server IP address with a default rate class (that can be overridden by individual virtual servers or iRules® later).

 ún Note

This example has a single virtual server IP, and it does not matter what interface the traffic is destined for. If you want to be more specific, you could specify each service port, as well (for example: HTTP, FTP, Telnet, and so on).

```plaintext
create packet-filter virtuals {
  order 20
  action accept
  vlan external
  rate-class root
  rule { ( dst host 172.19.254.80 )}
}
```
Options

You can use these options with the `packet-filter` component to create packet filter rules:

- **action**
  Specifies how the system handles a packet that matches the criteria in the packet filter rule. There is no default; you must specify a value when you create a packet filter rule.

  The possible values are:

  - **accept**
    Indicates that the system accepts the packet and stops processing additional packet filter rules, if there are any.

  - **continue**
    Indicates that the system acknowledges the packet for logging or statistical purposes, but makes no decision on how to handle the packet. The system continues to evaluate traffic matching a rule with the `continue` action, starting with the next packet filter rule in the list.

  - **discard**
    Indicates that the system drops the packet and stops processing additional packet filter rules, if there are any.

  - **reject**
    Indicates that the system drops the packet and sends a reject packet to the sender, indicating that the packet was refused.

- **description**
  User-defined description.

- **glob**
  Displays the items that match the `glob` expression. For a description of `glob` expression syntax, see the `glob` man page.

- **logging**
  Enables or disables packet filter logging. If you omit this value, no logging is performed.

- **name**
  Specifies a unique name for the component. This option is required for the commands `create`, `delete`, and `modify`.

- **order**
  Specifies a sort order greater than 0 (zero). No two rules can have the same sort order. There is a single, global list of rules. Each rule in the list has a relative integer order. The system first evaluates the rule with the lowest order value, and then evaluates all other rules based on ascent of the order value assigned to each rule.

  For example, if there are five rules, numbered 500, 100, 300, 200, 201; the rule evaluation order is 100, 200, 201, 300, 500.

  The system compares each packet to be filtered against the list of rules in sequence, starting with the first. Evaluation of the rule list stops on the first match that has an action of `accept`, `discard`, or `reject`. A match on a rule with an action of `none` does not stop further evaluation of the rule.
list; the system updates the statistics count and generates a log if the rule indicates it, but otherwise rule processing continues with the next rule in the list.

F5 Networks recommends that you sequence rules for effect and efficiency; generally this means:

- Assign the lowest order value to more specific rules, so that the system will evaluate those rules first.
- The system evaluates one expression with multiple criteria more efficiently than multiple expressions each with a single criterion.

This option is required.

◆ **rate-class**

  Specifies the name of a rate class. The value is the name of any existing rate class. If omitted, no rate filter is applied.

◆ **regex**

  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. For a description of regular expression syntax, see the `regex` man page.

◆ **rule**

  Specifies the BPF expression to match. The rule is mandatory, however, you can leave it empty. If empty, the packet filter rule matches all packets.

◆ **vlan**

  Specifies the VLAN to which the packet filter rule applies. The value for this option is any VLAN name currently in existence. If you omit this value, the rule applies to all VLANs. If you do not provide a VLAN name when you create a packet-filter, the rule applies to all VLANs.

**See also**

create, delete, edit, glob, list, ltm virtual, modify, net packet-filter-trusted, net rate-class, net vlan, net vlan-group, regex, reset-stats, show, tmsh
**packet-filter-trusted**

Modifies or displays trusted allow lists for packet filters.

**Module**

`net`

**Syntax**

Modify the `packet-filter-trusted` component within the `net` module using the following syntax.

```plaintext
modify packet-filter-trusted
  options:
    description [string]
    ip-addresses none
    ip-addresses [add | delete | replace-all-with] { [ip address ... ] }
    mac-addresses none
    mac-addresses [add | delete | replace-all-with] { [MAC address ... ] }
    vlans none
    vlans [add | delete | replace-all-with] { [vlan name ... ] }

edit packet-filter-trusted
```

**Display**

```plaintext
list packet-filter-trusted
show running-config packet-filter-trusted
  options:
    all-properties
    non-default-properties
    one-line
```

**Description**

You can use the `packet-filter-trusted` component to create a layer of security for the traffic management system using trusted allow lists.
**Trusted allow lists** are lists of IP addresses, MAC addresses, and VLANs that are exempt from packet filter rules.

**Important**

*By default, packet filtering is disabled. You must enable packet filtering using the Configuration utility. For more information, see the TMOS® Management Guide for BIG-IP® Systems.*

**Examples**

Creates a trusted allow list that allows anything listed to bypass the packet filter:

```
packet-filter-trusted {
  vlans add internal1 internal2
  mac-addresses add 00:02:3F:3E:2F:FE
}
```

In the above example, you have an administrative laptop that you want to have unrestricted access to the traffic management system. This is a laptop, and therefore it might have a different IP address from time to time. One way to solve the problem is to add a trusted MAC address. A **trusted MAC address** is a MAC address that passes MAC address-based authentication.

This trusted allow list example shows the laptop MAC address as **00:02:3F:3E:2F:FE**. Now the laptop can access the traffic management system regardless of what address it boots with or to which VLAN it is connected, as long as it is on the same physical segment as the traffic management system.

Also in this example, the traffic management system is configured with a basic firewall for the internal network. This example shows a way to filter incoming traffic and allow outgoing traffic to be unrestricted. To do this, you add trusted VLANs that represent all traffic that originated on the internal network. Another way to do this is to allow trusted IP addresses instead, for example: **192.168.26.0/24**.

**Options**

You can use these options with the `packet-filter-trusted` component to create trusted allow lists:

- **description**
  
  User-defined description.

- **ip-addresses**
  
  Specifies a list of source IP addresses. Any traffic matching a source IP address in the list is automatically allowed. This simplifies configuration of the packet filter to allow trusted internal traffic to be passed from VLAN to VLAN without a filter rule, including out to the Internet.
Processing of traffic by this option occurs before rule list evaluation, making it impossible to override this option and mask out (block) certain types of traffic with a packet filter rule. This option is empty by default.

- **mac-addresses**
  Specifies a list of MAC addresses. The system allows any traffic matching a MAC address in the source address list. This simplifies configuration of the packet filter to allow trusted internal traffic to be passed from VLAN to VLAN without a filter rule, including out to the Internet. Processing of traffic by this option occurs before rule list evaluation, making it impossible to override this option and mask out (block) certain types of traffic with a packet filter rule. This option is empty by default.

- **vlans**
  Specifies a list of ingress VLANs. Any traffic received on a VLAN that is on the ingress VLAN list is automatically allowed. This simplifies configuration of the packet filter to allow trusted internal traffic to be passed from VLAN to VLAN without a filter rule, including out to the Internet. Processing of traffic by this option occurs before rule list evaluation, making it impossible to override this option and mask out (block) certain types of traffic with a packet filter rule. This option is empty by default.

**See also**

edit, list, ltm virtual, modify, net packet-filter, net rate-class, net vlan, net vlan-group, show, tmsh
**port-mirror**

Configures interface (port) mirroring.

**Module**

net

**Syntax**

Modify the port-mirror component within the net module using the following syntax.

**Modify**

create port-mirror [interface_name]
modify port-mirror [interface_name]
  options:
  interfaces [add | default | replace-all-with] { [interface_name ... ] }
  interfaces [default | none]
edit port-mirror [ [ [interface_name] | [glob] | [regex] ] ... ]
  options:u
  all-properties

**Display**

list port-mirror
list port-mirror [ [ [interface_name] | [glob] | [regex] ] ... ]
show running-config port-mirror
show running-config port-mirror [ [ [interface_name] | [glob] | [regex] ] ... ]
  options:
  all-properties
  (default | exa | gig | kil | meg | peta | raw | tera | yotta | zetta)
  field-fmt

**Description**

You can use the port-mirror component to mirror traffic from interfaces on a blade to other interfaces on the same blade or another blade.
Examples

Creates a port mirror from interface 1.1 on blade 1 to interfaces 1.2, 1.3, 1.4 on the same blade. The system mirrors traffic from interfaces 1.2, 1.3, and 1.4 on blade 1 to interface 1.1 on the same blade:

```
create port-mirror 1/1.1 interfaces add 1/1.2 1/1.3 1/1.4
```

Deletes interfaces 1.3 and 1.4 on blade 1 from the existing port mirror 1/1.1 on the same blade:

```
modify port-mirror 1/1.1 interfaces delete 1/1.3 1/1.4
```

Options

You can use these options with the `port-mirror` component:

- **glob**
  Displays the items that match the `glob` expression. For a description of `glob` expression syntax, see the `glob` man page.

- **interface_name**
  Specifies the name of the interface, for example: 1/1.1.

- **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (`@[regular expression]`) to indicate that the identifier is a regular expression. For a description of regular expression syntax, see the `regex` man page.

See also

`create`, `delete`, `edit`, `glob`, `list`, `modify`, `net interface`, `regex`, `show`, `tmsh`
route

Configures a route for traffic management.

Module

net

Syntax

Configure the route component within the net module using the following syntax.

Create/Modify

create route [name]
modify route [name]

options:
  blackhole
  description [string]
  gw [ip address]
  interface [name]
  mtu [integer]
  network [ip address/netmask]
  pool [name]

edit route [ [name] | [glob] | [regex] ] ... ]

options:
  all-properties
  non-default-properties

Display

list route
list route [ [name] | [glob] | [regex] ] ... ]
show running-config route
show running-config route [ [name] | [glob] | [regex] ] ... ]

options:
  all-properties
  mtu
  non-default-properties
  one-line
  partition
Chapter 35

show route
show route
[ [name] | [glob] | [regex] ] ... ]
options:
  connected
  dynamic
  field-fmt
  lookup [ip address]
  static

Delete

deleate route [name]

Description

You can configure routes for the system, including default routes.

◆ Note

When you use the edit command to create a new route, by default the gw (gateway) option is set. If you do not want to use the gw option, remove that line of syntax in the editor.

Examples

Sets the route myRoute3 to the address 12.12.4.0/24 on the interface named external:
create route myRoute3 network 12.12.4.0/24 interface external

Displays the route that the system uses to reach the IP address 12.12.3.0:
show route lookup myRoute

Options

You can use the following options with the route component:

◆ Note

The blackhole, gw, interface, and pool options are mutually exclusive. You can use only one of these options at a time, and you must specify at least one of these options when configuring a route.

◆ blackhole
  Specifies that the system drops traffic that is addressed to the specified destination.
- **description**
  User-defined description.

- **connected**
  Displays connected routes.

- **dynamic**
  Displays dynamic routes.

- **glob**
  Displays the items that match the `glob` expression. For a description of `glob` expression syntax, see the `glob` man page.

- **gw**
  Specifies a gateway address for the system.

- **interface**
  Specifies the tunnel, VLAN, or VLAN group to which the system sends traffic.

- **ip address/netmask**
  Specifies the destination subnet and mask using CIDR notation, such as `12.12.3.0/24`. You can also specify the keyword `default` or `default-inet6`.

- **lookup**
  Displays the route that the system uses to reach the specified IP address. You can specify only a single IP address with the `lookup` option.

- **mtu**
  Sets a specific maximum transition unit (MTU). If you set this option to 0 (zero), the system selects the appropriate MTU for the route and does not display the MTU.

- **network**
  Specifies the destination subnet and mask using CIDR notation, such as `12.12.3.0/24`. You can also specify the keyword `default` or `default-inet6`.

- **pool**
  Specifies a pool to which the system sends traffic. This allows the system to send traffic to multiple, load-balanced gateways.

- **partition**
  Displays the administrative partition within which the route resides.

- **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (`@[regular expression]`) to indicate that the identifier is a regular expression. For a description of regular expression syntax, see the `regex` man page.

- **static**
  Displays static routes.

---

**See also**

- create, delete, edit list, ltm pool, modify, net vlan, net vlan-group, show, regex, tmsh
route-domain

Configures route-domains for traffic management.

Module

net

Syntax

Configure the route-domain component within the net module using the following syntax.

Create/Modify

create route-domain [ [name] | none]
modify route-domain [name]
  options:
    description [string]
    id [integer]
    parent [ [name] | none]
    strict [enabled | disabled]
    vlans [add | delete | replace-all-with] { [vlan name ... ] }
edit route-domain [ [name] | [glob] | [regex] ] ... ]
  options:
    all-properties
    non-default-properties

Display

list route-domain
list route-domain [ [name] | [glob] | [regex] ] ... ]
show running-config route-domain
show running-config route-domain [ [name] | [glob] | [regex] ] ... ]
  options:
    all-properties
    non-default-properties

Delete

delete route-domain [name]
Description

Using route domains, you can assign the same IP address to more than one device on a network, as long as each instance of the IP address resides in a separate routing domain.

Examples

Creates a route domain named myRouteDomain with an ID of 1 that includes my_vlan:

create route-domain myRouteDomain id 1 vlans add { my_vlan }

Displays all properties of all route domains:

list route-domain all-properties

Options

You can use the following options with the route-domain component:

- **description**
  Use defined description.

- **id**
  Specifies a unique numeric identifier for the route-domain. This option is required.

- **parent**
  Specifies the route domain the system searches when it cannot find a route in the configured domain. The default value is None.

  If you specify a parent, during route table lookup, if the system cannot find a route in the current route domain, the system searches routes in the parent route domain. If no route is found in the parent route domain, the system searches the parent route domain's parent, and so on, until the system finds either a match or a parent with a value of None.

  For example, if rd_1 has a parent of rd_0 (in this example, route domain rd_0 has a parent of None), and you include vlan_a in rd_1, when requests arrive for vlan_a, the system looks in rd_1 for a route for the specified destination. If no route is found, the system searches route domain 0. If it still cannot find a route, the request for vlan_a fails. If, using the same example, you set the parent to None, under the same conditions, the system looks in rd_1, and if it cannot find a matching route, the system refrains from searching any other route domain, the request for vlan_a fails.

- **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. For a description of regular expression syntax, see the regex man page.
◆ **strict**
   Specifies whether the system allows a connection to span route domains. The default value is `enabled`. 
   
   *Note:* When you enable this option, the system can find invalid iRules that passed validation.

◆ **vlans**
   Specifies VLANs, by name, for the system to use in the route domain. The default value is `none`.

### See also

`create`, `delete`, `edit`, `glob`, `list`, `modify`, `net vlan`, `net vlan-group`, `regex`, `show`, `tmsh`
router-advertisement

Configures IPv6 prefixes for router advertisement on a VLAN.

Module

net

Syntax

Modify the `router-advertisement` component within the `net` module using the following syntax.

Modify

create router-advertisement [name]
modify router-advertisement [name]

options:
  current-hop-limit [integer]
  description [string]
  disabled | enabled
  max-interval [integer]
  min-interval [integer]
  mtu [integer]
  no-other-config | other-config

prefixes
  [add | delete | modify | replace-all-with] {
    [name] ... {
      autonomous | not-autonomous
      description [string]
      on-link | not-on-link
      preferred-lifetime [integer]
      prefix [ip address]
      prefix-length [integer]
      valid-lifetime [integer]
    }
  }
  reachable-time [integer]
  retransmit-timer [integer]
  router-lifetime [integer]
  unmanaged | managed
  vlan [name]

edit router-advertisement [ [ [name] | [glob] | [regex] ] ... ]

options:
all-properties
non-default-properties

Display

list router-advertisement
list router-advertisement [ [ [name] | [glob] | [regex] ] ... ]
show running-config router-advertisement
show running-config router-advertisement
[ [ [name] | [glob] | [regex] ] ... ]
options:
  all-properties
  non-default-properties
  one-line

Delete

delete router-advertisement [name]

Description

Router advertisements are part of the configuration of BIG-IP network components. When creating a router advertisement, you must specify a VLAN on the command line.

Examples

Creates the router advertisement my_ra that includes the VLAN my_vlan:
create router-advertisement my_ra vlan my_vlan

Deletes the router advertisement named my_ra and all associated prefixes:
delete router-advertisement my_ra

Options

Note the following information regarding options for the router-advertisement component:

- The options disabled and enabled are mutually exclusive.
- The options no-other-config and other-config are mutually exclusive.
- The options unmanaged and managed are mutually exclusive.
- The options autonomous and not-autonomous are mutually exclusive.
- The options on-link and not-on-link are mutually exclusive.
You can use these options with the `router-advertisement` component:

- **autonomous**
  Indicates that the Autonomous Flag field in the prefix information option be set to 1. The default value is 1.

- **current-hop-limit**
  Defines the hop limit sent in the router advertisement. The default value is 0 (zero).

- **description**
  User-defined description.

- **disabled**
  Disables router advertisement for the VLAN. This is the default.

- **enabled**
  Enables router advertisement for the VLAN.

- **glob**
  Displays the items that match the `glob` expression. See `help glob` for a description of `glob` expression syntax.

- **managed**
  Indicates that the Managed address configuration flag field in the router advertisement is set to 1.

- **max-interval**
  Specifies the maximum time allowed between sending unsolicited multicast Router Advertisements from the interface, in seconds. The default value is 600.

- **min-interval**
  Specifies, in seconds, the minimum time allowed between sending unsolicited multicast Router Advertisements from the interface. The default value is 200.

- **mtu**
  Sets a specific maximum transition unit (MTU) for the VLAN. The default value is 0 (zero).

- **name**
  Specifies a unique name for the component. This option is required for the `create`, `delete`, and `modify` commands.

- **no-other-config**
  Indicates that the Other Configuration flag field in the router advertisement is set to 0 (zero). The default value is 0 (zero).

- **not-autonomous**
  Indicates that the Autonomous flag field in the prefix information option is set to 0 (zero).

- **not-on-link**
  Indicates that the on-link flag field in the prefix information option is set to 0 (zero).

- **on-link**
  Indicates that the on-link flag field in the prefix information option is set to 1. The default value is 1.
other-config
Indicates that the Other Configuration flag field in the router advertisement is set to 1.

preferred-lifetime
Specifies, in seconds, the value for the Preferred Lifetime field in the prefix information option. The default value is 604800.

prefix
Specifies the prefix for the prefix information option.

prefix-length
Specifies the length of the prefix for the prefix information option.

prefixes
Specifies the objects that hold the prefix specific information for the router advertisement.

reachable-time
Specifies the value to be used for the Reachable Time field in the Router Advertisement. The default value is 0 (zero).

regex
Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. For a description of regular expression syntax, see the regex man page.

retransmit-timer
Specifies the value to be used for the Retransmit Timer field in the Router Advertisement. The default value is 0 (zero).

router
Specifies that the router advertisement acts as a router for the VLAN.

router-lifetime
Specifies the value to be used for the Router Lifetime field in the Router Advertisement. The default value is 1800.

unmanaged
Specifies that the Managed address configuration flag field in the router advertisement is set to 0 (zero). The default value is 0 (zero).

valid-lifetime
Specifies, in seconds, the value for the Valid Lifetime field in the prefix information option. The default value is 2592000.

See also
create, delete, edit, glob, list, modify, net interface, regex, show, tmsh
rst-cause

Displays and resets TCP/IP Reset Cause Statistics.

Module

net

Syntax

Display and reset the rst-cause component within the net module using the syntax in the following section.

Modify

reset-stats rst-cause

Display

show rst-cause
  options:
    (default | field-fmt)

Description

You can use the rst-cause component to display and reset TCP/IP reset cause statistics. This will help to debug the reason for TCP/IP reset.

Options

For information about the options that you can use with the command show, see help show.

See also

reset-stats, show, tmsh
**self**

Configures a self IP address for a VLAN.

**Module**

net

**Syntax**

Modify the self component within the net module using the following syntax.

**Create/Modify**

create self [name]
modify self [name]

options:

- address [ip address/netmask]
- allow-service [ all | default | none ]
- allow-service [add | delete | replace-all-with] { [protocol:port] ... }
- description [string]
- traffic-group [string]
- floating [disabled | enabled]
- unit [integer]
- vlan [name]

edit self [ [ [ip address/mask] | [glob] | [regex] ] ... ]

options:

- all-properties
- non-default-properties

**Display**

list self
list self [ [name] | [glob] | [regex] ] ... ]

show running-config self
show running-config self [ [name] | [glob] | [regex] ] ... ]

options:

- all-properties
- non-default-properties

**Delete**

delete self [ip address/mask]
Description

A self IP address is an IP address that is assigned to the system. Self IP addresses are part of the configuration of the BIG-IP network components. You must define at least one self IP address for each VLAN.

Examples

Adds the self IP address 10.10.10.24 to the VLAN named internal. This entry is named mySelf. Alternatively, the name can encompass the ip address and mask fields, like the following example.

create self mySelf address 10.10.10.24/16 vlan internal

Creates the self IP address 10.10.10.24 for the VLAN named internal:

create self 10.10.10.24 vlan internal

Enables a floating IP address on the external VLAN. The traffic-group option makes this virtual address available to whichever device is active on the given traffic-group. In other words, when the standby device becomes the active device for that traffic-group, it uses this virtual address. Only one of the devices in the traffic-group can use the IP address at any given time.

modify self 10.1.1.24 vlan external traffic-group /Common/traffic-group-1>

Options

You can use the following options with the self component:

- **allow-service**
  Specifies the type of protocol/service that the VLAN handles.
  The options are:
  - **add**
    Adds the specified protocol/service to the VLAN.
  - **all**
    Specifies that the VLAN handles all protocols/services.
  - **default**
    Specifies that the system uses the default value, which is none.
  - **delete**
    Removes the specified protocol/service from the VLAN.
  - **none**
    Specifies that the VLAN handles no protocols/services.
  - **replace-all-with**
    Replaces the current protocol/service that the VLAN handles with the specified protocol/service.
◆ **floating**
Read-only property based on the **traffic-group**. A floating self IP address is a self IP address for a VLAN that serves as a shared address by all devices of a BIG-IP traffic-group.

◆ **address**
Specifies the IP address and netmask to be assigned to the system. This is an optional field; if not specified, the name of the entry needs to be in the format `[ip address/mask]`.

◆ **description**
User-defined description.

◆ **glob**
Displays the items that match the **glob** expression. For a description of **glob** expression syntax, see the **glob** man page.

◆ **ip address/mask**
Specifies the self IP address and netmask for the VLAN. This option is required.

◆ **regex**
Displays the items that match the regular expression. The regular expression must be preceded by an at sign (`@[regular expression]`) to indicate that the identifier is a regular expression. For a description of regular expression syntax, see the **regex** man page.

◆ **unit**
Read-only property that specifies the unit in a redundant system. Based on **traffic-group**.

◆ **traffic-group**
Specifies the traffic group of the self IP address. The default traffic group is **traffic-group-local-only**, the non-floating traffic-group.

◆ **inherited-traffic-group**
Read-only property that indicates if the **traffic-group** is inherited from the parent folder.

◆ **vlan**
Specifies the VLAN for which you are setting a self IP address. This option is required.

---

**See also**

create, delete, edit, glob, list, modify, net vlan, net vlan-group, regex, show, tmsh
self-allow

Configures the default allow list for all self IP addresses on the BIG-IP system when the option allow-service of the component self is set to default.

Module

net

Syntax

Modify the self-allow component within the net module using the following syntax.

Modify

modify self-allow
options:
  defaults [all | none]
  defaults [add | delete | replace-all-with] { [protocol:port ... ] }

edit self-allow
options:
  all-properties

Display

list self-allow

show running-config self-allow
options:
  all-properties
  defaults
  one-line

Delete

You cannot delete the default allow list.

Description

You can use the self-allow component to modify or display the default allow list for all self IP addresses on the BIG-IP system when the allow-service option of the self component is set to default. The default
allow list displays which service and protocol ports allow connections from outside the system. The system refuses connections made to a service or protocol port that is not on the list.

Examples

Sets the default allow list for all self IP addresses on the system to the system default:

```bash
modify self-allow defaults all
```

Sets the default allow list for all self IP addresses on the system to TCP:

```bash
modify self-allow default replace-all-with { tcp:55 }
```

Displays the default allow list for all self IP addresses on the system:

```bash
list self-allow defaults
```

Options

You can use the following option with the `self-allow` component:

**defaults**

Sets the default allow list to one of the following:

- **all**
  Specifies that all protocols and services allow connections from outside the system. Use this option to open the system to complete access.

- **none**
  Specifies that no protocols or services allow connections from outside the system.

- **protocol:port**
  Specifies a list of protocols and services that allow connections from outside the system.

- **replace-all-with**
  Replaces the current protocols and services that allow connections from outside the system with the specified protocols and services.

See also

`edit`, `list`, `modify`, `net vlan`, `net vlan-group`, `show`, `tmsh`
**stp**

Configures a Spanning Tree Protocol (STP) instance.

**Module**

```
net
```

**Syntax**

Configure the stp component within the net module using the following syntax.

**Create/Modify**

```
create stp [all | [name] ]
modify stp [all | [name] ]
```

options:

```
interfaces [add | delete | modify | replace-all-with] { [interface name] {
    options:
    
    external-path-cost [integer]
    internal-path-cost [integer]
    priority [integer]

    }

    interfaces none

    priority [integer]

    trunks [add | delete | modify | replace-all-with] { [interface name] {
    options:
    
    external-path-cost [integer]
    internal-path-cost [integer]
    priority [integer]

    }

    trunks none

    vlans [add | delete | replace-all-with] { [vlan name ... ] }

    vlans none

    edit stp [ [ all | [name] | [glob] | [regex] ] ... ]
```

options:

```
all-properties
non-default-properties
```
Chapter 35

Display

list stp
list stp [ [ all | [name] | [glob] | [regex] ] ... ]
show running-config stp
show running-config stp [ [ all | [name] | [glob] | [regex] ] ... ]

options:

all-properties
non-default-properties

Delete

delete stp [all | [name] ]

Description

You can use the stp component to configure an STP instance.

Examples

Displays all STP instances on the system:
list stp

Displays the running configuration information for all STP instances:
show running-config stp

Removes all members from the STP instance and then deletes the instance itself. Note that you cannot delete spanning tree instance 0 (the Common and Internal Spanning Tree). You can only use the delete command in Multiple Spanning Tree Protocol (MSTP) mode:
delete stp myStp2

Options

You can use these options with the stp component:

◆ description
User-defined description.

◆ external-path-cost
Specifies the external path cost number for either an interface or trunk. The default value is 20000.

Each network interface has an associated path cost within each spanning tree instance. The path cost represents the relative cost of sending network traffic through that interface. In calculating the spanning tree, the algorithm tries to minimize the total path cost between each point of the tree and the root bridge. By manipulating the path costs of different
interfaces or trunks it is possible to steer traffic toward paths that are faster, more reliable, or more economical. Path costs can take values in the range \(1 - 200,000,000\). The default path cost for an interface or a trunk is based on the maximum, not actual speed, of the interface or trunk.

In MSTP mode there are two kinds of path cost: external and internal. The external path cost applies only to spanning tree instance 0, the Common and Internal Spanning Tree (CIST). It is used to calculate the cost to reach an adjacent spanning tree region.

- **glob**
  Displays the items that match the glob expression. For a description of glob expression syntax, see the glob man page.

- **internal-path-cost**
  Specifies the internal path cost number for either an interface or trunk. The default value is 20000.

  Each network interface has an associated path cost within each spanning tree instance. The path cost represents the relative cost of sending network traffic through that interface. In calculating the spanning tree, the algorithm tries to minimize the total path cost between each point of the tree and the root bridge. By manipulating the path costs of different interfaces or trunks it is possible to steer traffic toward paths that are faster, more reliable, or more economical. Path costs can take values in the range \(1 - 200,000,000\). The default path cost for an interface or a trunk is based on the maximum, not actual speed, of the interface or trunk.

In MSTP mode there are two kinds of path cost: external and internal. The internal path costs can be independently set for each spanning tree instance (including instance 0) in MSTP mode. The internal path costs are used to calculate the costs of reaching adjacent bridges within the same spanning tree region.

- **priority**
  Specifies the priority number of either a bridge, interface, or trunk. The default value for a bridge is 61440. The default value for both interfaces and trunks is 128.

  Each bridge, interface, and trunk in a spanning tree instance has a priority value. The relative values of the priorities control the topology of the spanning tree chosen by the protocol. The bridge with the lowest priority value (numerically) will become the root of the spanning tree. Priority values vary from 0 - 61440 in steps of 4096.

- **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. For a description of regular expression syntax, see the regex man page.

- **vlans**
  Specifies the VLANs that you want to add to, delete from, or replace-all-with for this STP instance.
See also

create, delete, edit, glob, list, modify, net interface, net trunk, net vlan, regex, show, tmsh
**stp-globals**

Configures spanning tree protocols on the system.

**Module**

```text
net
```

**Syntax**

Configure the `stp-globals` component within the `net` module using the following syntax.

**Modify**

```text
modify stp-globals
  options:
    config-name [name]
    config-revision [integer]
    description [string]
    fwd-delay [integer]
    hello-time [integer]
    max-age [integer]
    max-hops [integer]
    mode [disabled | mstp | passthru | rstp | stp]
    transmit-hold [integer]
```

```text
edit stp-globals
  options:
    all-properties
    non-default-properties
```

**Display**

```text
list stp-globals
show running-config stp-globals
  options:
    all-properties
    non-default-properties
    one-line
```
Description

Provides the ability to configure spanning tree protocols for the traffic management system. Spanning tree protocols are Layer 2 protocols for preventing bridging loops. The system supports multiple spanning tree protocol (MSTP), rapid spanning tree protocol (RSTP), and spanning tree protocol (STP).

Examples

Sets the STP mode to **passthru**. Passthru mode forwards spanning tree bridge protocol data units (BPDUs) received on any interface to all other interfaces:

```plaintext
modify stp-globals mode passthru
```

Sets the STP mode to **disabled**. No MSTP, RSTP, or STP packets are transmitted or received on the interface or trunk, and the spanning tree algorithm exerts no control over forwarding or learning on the port or the trunk:

```plaintext
modify stp-globals mode disabled
```

Options

You can use these options with the `stp-globals` component:

- **config-name**
  Specifies the configuration name (1 - 32 characters in length) only when the spanning tree mode is MSTP. The default configuration name is a string representation of a globally unique MAC address belonging to the traffic management system.

  The MSTP standard introduces the concept of spanning tree regions, which are groups of adjacent bridges with identical configuration names, configuration revision levels, and assignments of VLANs to spanning tree instances.

- **config-revision**
  Specifies the revision level of the MSTP configuration only when the value of the `mode` option is `mstp`. The specified number must be in the range 0 to 65535. The default value is 0 (zero).

- **description**
  User-defined description.

- **fwd-delay**
  In the original STP, the forward delay parameter controlled the number of seconds for which an interface was blocked from forwarding network
traffic after a reconfiguration of the spanning tree topology. This parameter has no effect when RSTP or MSTP are used, as long as all bridges in the spanning tree use the RSTP or MSTP protocol. If any legacy STP bridges are present, then neighboring bridges must fall back to the old protocol, whose reconfiguration time is affected by the value of the `fwd-delay` option. The default value is 15 seconds, and the valid range is 4 to 30.

◆ **hello-time**
Specifies the time interval in seconds between the periodic transmissions that communicate spanning tree information to the adjacent bridges in the network. The default value is 2 seconds, and the valid range is 1 to 10. The default value is optimal in virtually all cases. F5 Networks recommends that you do not change the value of the **hello-time** option.

◆ **max-age**
Specifies the number of seconds for which spanning tree information received from other bridges is considered valid. The default value is 20 seconds, and the valid range is 6 to 40 seconds.

◆ **max-hops**
Specifies the maximum number of hops an MSTP packet can travel before it is discarded. Use this option only when the value of the **mode** option is **mstp**. The number of hops must be in the range of 1 to 255 hops. The default number of hops is 20.

◆ **mode**
Specifies one of three spanning tree modes:
- **disabled**
  Discards spanning tree bridge protocol data units (BPDUs) received on any interface.
- **mstp**
  Specifies multiple spanning tree protocol.
- **passthru**
  Forwards spanning tree bridge protocol data units (BPDUs) received on any interface to all other interfaces. Essentially, **passthru** mode makes the traffic management system transparent to spanning tree BPDUs. This is the system default.
- **rstp**
  Specifies rapid spanning tree protocol (RSTP), which converges to a fully connected state quickly.
- **stp**
  The system supports STP mode for legacy systems. If STP is detected in the network, the traffic management system changes to STP mode, even when the **mode** option is set to **disabled**, **mstp**, or **rstp**.

◆ **transmit-hold**
Specifies the absolute limit on the number of spanning tree protocol packets the traffic management system might transmit on a port in any **hello-time** interval. It is used to ensure that spanning tree packets do not unduly load the network, even in unstable situations. The default value is 6 packets, and the valid range is 1 to 10 packets.
See also

edit, interface, list, modify, show, tmsh
trunk

Configures a trunk with link aggregation.

Module

net

Syntax

Modify the trunk component within the net module using the following syntax.

Create/Modify

create trunk [name]
modify trunk [name]
  options:
    bandwidth
    description [string]
    distribution-hash [dst-mac | src-dst-ip | src-dst-mac]
    interfaces [add | delete | replace-all-with] { [name ... name] }
    lacp [disabled | enabled]
    lacp-mode [active | passive]
    lacp-timeout [short | long]
    link-select-policy [auto | maximum-bandwidth]
    mac-address [MAC Address]
    stp [disabled | enabled]
    stp-reset
edit trunk [ [ [name] | [glob] | [regex] ] ... ]
  options:
    all-properties
    non-default-properties
reset-stats trunk
reset-stats trunk [ [ [name] | [glob] | [regex] ] ... ]

Display

list trunk
list trunk [ [ [name] | [glob] | [regex] ] ... ]
show running-config trunk
show running-config trunk [ [ [name] | [glob] | [regex] ] ... ]
  options:
    all-properties
Link aggregation allows multiple physical links to be treated as one logical link. It is also referred to as trunking.

The main objective of link aggregation is to provide increased bandwidth at a lower cost, without having to upgrade hardware. The bandwidth of the aggregated trunk is the sum of the capacity of individual member links. Thus, it provides an option for linearly incremental bandwidth as opposed to bandwidth options available through physical layer technology. The traffic management system supports link aggregation control protocol (LACP).

When a trunk is created, LACP is disabled by default. In this mode, no control packets are exchanged and the member links carry traffic as long as the physical layer is operational. In the event of physical link failure, an LACP member is removed from the aggregation.

Both endpoints of the trunk must have identical LACP configuration to work properly. A mixed configuration, where one endpoint is LACP enabled and the other is LACP disabled, is not valid.

Examples

Creates a trunk named my_trunk that includes the interfaces 1.1, 1.2, and 1.3:

```
create trunk my_trunk interfaces add 1.1 1.2 1.3
```

Enables LACP on the trunk named my_trunk:

```
modify trunk my_trunk lACP enabled
```

Enables active LACP mode on the trunk my_trunk:

```
modify trunk my_trunk lACP-mode active
```
Options

You can use these options with the `trunk` component:

- **bandwidth**
  Specifies the operational bandwidth in bytes per second.

- **cfg-mbr-count**
  Displays the number of configured members associated with this trunk.

- **distribution-hash**
  Specifies the basis for the hash that the system uses as the frame distribution algorithm. The system uses the resulting hash to determine which interface to use for forwarding traffic.

  When frames are transmitted on a trunk, they are distributed across the working member links. The distribution function ensures that the frames belonging to a particular conversation are neither mis-ordered nor duplicated at the receiving end. Distribution is done by calculating a hash value based on source and destination addresses carried in the frame, and associating the hash value with a link. All frames with a particular hash value are transmitted on the same link, thereby maintaining frame order.

  The options are:
  - **dst-mac**
    Uses the destination and MAC addresses to calculate the hash value.
  - **src-dst-mac**
    Uses the source, destination, and MAC addresses to calculate the hash value.
  - **src-dst-ip**
    Uses the source, destination, MAC, and IP addresses to calculate the hash value.

- **glob**
  Displays the items that match the `glob` expression. For a description of `glob` expression syntax, see the `glob` man page.

- **id**
  Displays the ID of the trunk.

- **interfaces**
  Specifies the interfaces by name separated by spaces that you want to add to the trunk, delete from the trunk, or with which you want to replace all existing interfaces associated with the trunk.

- **lacp**
  Specifies, when enabled, that the system supports the link aggregation control protocol (LACP), which monitors the trunk by exchanging control packets over the member links to determine the health of the links. If LACP detects a failure in a member link, it removes the link from the link aggregation. LACP is disabled by default, for backward compatibility.
◆ **lacp-mode**  
Specifies the operation mode for LACP, if the `lacp` option is enabled for the trunk.

The options are:

- **active**  
  Specifies that the system periodically transmits LACP packets, regardless of the control value of the peer system.

- **passive**  
  Specifies that the system periodically transmits LACP packets, unless the mode of the peer system is **active**.

◆ **lacp-timeout**  
Specifies the rate at which the system sends the LACP control packets.  
The default value is **long**.

The options are:

- **long**  
  Specifies that the system exchanges LACP packets every 30 seconds.

- **short**  
  Specifies that the system exchanges LACP packets every one second.

◆ **link-select-policy**  
Sets the LACP policy that the trunk uses to determine which member link (interface) can handle new traffic.

Link aggregation is allowed only when all the interfaces are operating at the same media speed and connected to the same partner aggregation system. When there is a mismatch among configured members due to configuration errors or topology changes (auto-negotiation), link selection policy determines which links become working members and form the aggregation.

The options are:

- **auto**  
  Specifies that the system chooses the lowest numbered operational link as the reference link. All the members that have the same media speed and are connected to the same partner as that of the reference link are declared as working members, and they are aggregated. The other configured members do not carry traffic.

- **maximum-bandwidth**  
  Specifies that the system adds to the aggregation a subset of links that gives maximum aggregate bandwidth to the trunk.

◆ **mac-address**  
Specifies the media access control (MAC) address, which is associated with the trunk, in not case-sensitive hexadecimal colon notation, for example: `00:0b:09:88:00:9a`.

◆ **media**  
Displays the media settings for the trunk.

◆ **name**  
Specifies a unique name for the component. This option is required for the commands `create`, `delete`, and `modify`.  

- **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. For a description of regular expression syntax, see the `regex` man page.

- **stp**
  Enables or disables spanning tree protocols (STP). If you disable STP, the system does not transmit or receive STP, RSTP, or MSTP packets on the trunk, and STP has no control over forwarding or learning on the trunk. The default value is `enabled`.

- **stp-reset**
  Resets STP, which forces a migration check.

- **working-mbr-count**
  Displays the number of working members associated with this trunk.

**See also**

`create`, `delete`, `edit`, `glob`, `list`, `modify`, `net interface`, `net vlan`, `net vlan-group`, `regex`, `reset-stats`, `show`, `tmsh`
Chapter 35

vlan

Configures a virtual local area network (VLAN).

Module

net

Syntax

Modify the vlan component within the net module using the following syntax.

Create/Modify

create vlan [name]
modify vlan [name]

options:
  auto-lasthop [default | enabled | disabled]
  description [string]
  failsafe [disabled | enabled]
  failsafe-action [failover | failover-restart-tm | go-active | reboot | restart]
  failsafe-timeout [integer]
  interfaces [add | delete | modify | replace-all-with] {
    [name ... name] {
      [tagged | untagged]
    }
  }
  interfaces none
  learning [disable-drop | disable-forward | enable-forward]
  mac-masquerade [MAC address]
  mtu [integer]
  source-checking [disabled | enabled]
  tag [integer]
edit vlan [ [ [name] | [glob] | [regex] ] ... ]

options:
  all-properties
  non-default-properties

Display

list vlan
list vlan [ [ [name] | [glob] | [regex] ] ... ]
show running-config vlan
show running-config vlan [ [ [name] | [glob] | [regex] ] ... ]
**Options**

You can use these options with the `vlan` component:

- **description**
  
  User-defined description.

---

**Delete**

```
delete vlan [name]
```
◆ **failsafe**
Enables or disables a fail-safe mechanism that causes the active unit in a redundant system to fail over to the standby unit when loss of traffic is detected on a VLAN, and the system does not restore traffic during the failover timeout period for that VLAN. The default value is disabled. When you set the VLAN **failsafe** option to enabled, the default **failsafe-action** value is restart-all. Therefore, when the fail-safe mechanism is triggered, all the daemons are restarted and the unit fails over.

◆ **failsafe-action**
Specifies the action for the system to take when the fail-safe mechanism is triggered. The default value is failover-restart-tm.

◆ **failsafe-timeout**
Specifies the number of seconds that an active unit can run without detecting network traffic on this VLAN before it starts a failover. The default value is 90 seconds.

◆ **glob**
Displays the items that match the **glob** expression. For a description of **glob** expression syntax, see the **glob** man page.

◆ **interfaces**
Specifies a list of tagged or untagged interfaces and trunks that you want to configure for the VLAN. Use tagged interfaces or trunks when you want to assign a single interface or trunk to multiple VLANs.

A **tagged interface** is one that you assign to a VLAN in a way that causes the system to add a VLAN tag into the header of any frame passing through that interface or trunk.

A **trunk** is a combination of two or more interfaces and cables configured as one link.

◆ **learning**
Specifies whether switch ports placed in the VLAN are configured for switch learning, forwarding only, or dropped. The default value is enable-forward.

◆ **mac-masquerade**
Configures a shared MAC masquerade address. The default value is 0:0:0:0:0:0.

You can share the media access control (MAC) masquerade address between units in a redundant system. This has the following advantages:

- Increased reliability and failover speed, especially in lossy networks
- Interoperability with switches that are slow to respond to the network changes
- Interoperability with switches that are configured to ignore network changes

◆ **mtu**
Sets a specific maximum transition unit (MTU) for the VLAN. The default value is 1500.
◆ **name**
   Specifies a unique name for the component. This option is required for the commands **create**, **delete**, and **modify**.

◆ **regex**
   Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. For a description of regular expression syntax, see the **regex** man page.

◆ **source-checking**
   Specifies that only connections that have a return route in the routing table are accepted. The default value is **disabled**.

◆ **tag**
   Specifies a number that the system adds into the header of any frame passing through the VLAN. The value can be 1 through 4094. The default value is to not use this option, and the system assigns a tag number.

**See also**

create, delete, edit, glob, list, ltm virtual, modify, net interface, net self, net vlan-group, regex, show, tmsh
Chapter 35

**vlan-allowed**

Displays a list of available VLANs which can be used by the system.

**Module**

net

**Syntax**

Modify the `vlan-allowed` component within the `net` module using the syntax shown in the following sections.

**Display**

```plaintext
show vlan-allowed
  options:
    field-fmt
```

**Description**

Displays a list of available VLANs which can be used by the system.

**See also**

`tmsh`
vlan-group

Configures a VLAN group.

Module

net

Syntax

Modify the vlan-group component within the net module using the following syntax.

Create/Modify

create vlan-group [name]
modify vlan-group [name]
options:
  auto-lasthop [default | enabled | disabled]
  bridge-in-standby [disabled | enabled]
  bridge-multicast [disabled | enabled]
  bridge-traffic [disabled | enabled]
  description [string]
  mac-masquerade [mac address]
  members [add | delete | replace-all-with] { [vlan name] ... }
  members [default | none]
  mode [opaque | translucent | transparent]
  proxy-excludes [add | default | delete | replace-all-with] { [ip address] ... }
  proxy-excludes [default | none]
  tag [integer]
edit vlan-group [ [ [name] | [glob] | [regex] ] ... ]
options:
  all-properties
  non-default-properties

Display

list vlan-group
list vlan-group [ [ [name] | [glob] | [regex] ] ... ]
show running-config vlan-group
show running-config vlan-group [ [ [name] | [glob] | [regex] ] ... ]
options:
  all-properties
  non-default-properties
Chapter 35

```
one-line
show vlan-group
show vlan-group [ [ [name] | [glob] | [regex] ] ... ]
  options:
    all-properties
    (default | exa | gig | kil | meg | peta | raw | tera | yotta | zetta)
field-fmt

Delete

delete vlan-group [name]

Description

You can use the `vlan-group` component to define a VLAN group, which is a grouping of two or more VLANs belonging to the same IP network for the purpose of allowing Layer 2 packet forwarding between those VLANs. The VLANs between which the packets are to be passed must be on the same IP network, and they must be grouped using the `vlan-group` component. For example:

```
modify vlan-group network11 members add internal external
```

Examples

You can use these options with the `vlan-group` component:

- **bridge-traffic**
  When enabled, specifies that the VLAN group forwards all frames, including non-IP traffic. The default value is `disabled`.

- **bridge-in-standby**
  When enabled, specifies that the VLAN group forwards packets, even when the system is the standby unit in a redundant system. This option is
designated for deployments in which the VLAN group exists on only one of the units. If that does not match your configuration, using this option can cause adverse effects. The default value is enabled.

- **bridge-multicast**
  When enabled, allows bridging of non-Internet Protocol (IP) Address Resolution Protocol (ARP) multicast frames across a VLAN group. An example of when you might want to use this option is when you are implementing the spanning tree protocol (STP).

- **description**
  User-defined description.

- **glob**
  Displays the items that match the `glob` expression. For a description of `glob` expression syntax, see the `glob` man page.

- **mac-masquerade**
  Specifies a MAC address to be used with a redundant system. This is a 6-byte Ethernet address in not case-sensitive hexadecimal colon notation, for example: `00:0b:09:88:00:9a`.

- **members**
  The names of the VLANs that you want to add to or delete from the VLAN group.

- **migration-keepalive**
  Specifies whether the system will send keepalive frames (TCP keepalives and empty UDP packets depending on the connection type) when a node is moved from one VLAN group member to another VLAN group member for all existing connections that the system has to that node.

- **mode**
  Specifies the level of exposure of remote MAC addresses within VLAN groups. The default value is translucent. The options are:
  - **opaque**
    Use this option when you have a Cisco router in the network sending CDP packets to the system. Because opaque VLAN groups require a source and destination MAC address, and CDP packets do not contain a source and destination MAC address, the CDP packets are not forwarded through the VLAN group. This mode changes the MAC address to the MAC address assigned to the VLAN group, a proxy ARP with Layer 3 forwarding.
  - **translucent**
    Use the real MAC address of the requested host with the locally-unique bit toggled. Specifies that the system uses Layer 2 forwarding with the locally-unique bit toggled in ARP responses across VLANs.
  - **transparent**
    Leaves the MAC address unchanged by the traffic management system. Specifies that the system uses Layer 2 forwarding with the original MAC address of the remote system preserved across VLANs.
◆ **name**
  Specifies a unique name for the component. This option is required for the commands `create`, `delete`, and `modify`.

◆ **proxy-excludes**
  Specifies the IP addresses that you want to include in the proxy ARP exclusion list. If you use VLAN groups, you must configure a proxy ARP forwarding exclusion list. F5 Networks recommends that you configure this feature if you use VLAN groups with a redundant system. The reason is that both units need to communicate directly with their gateways and the back-end nodes. Creating a proxy ARP exclusion list prevents traffic from being sent through the active unit due to proxy ARP. This traffic needs to be sent directly to the destination.

◆ **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. For a description of regular expression syntax, see the `regex` man page.

◆ **tag**
  Specifies a number from 1 through 4094 to be the tag for the VLAN. A **VLAN tag** is an identification number the system inserts into the header of a frame that indicates the VLAN to which the destination device belongs. Use VLAN tags when a single interface forwards traffic for multiple VLANs.

**See also**

`create`, `delete`, `edit`, `glob`, `list`, `modify`, `net interface`, `net self`, `net vlan`, `net virtual`, `regex`, `show`, `tmsh`
**wccp**

Configures Web Cache Communication Protocol (WCCP) services.

**Module**

**net**

**Syntax**

Configure the `wccp` component within the `net` module using the following syntax.

**Create/Modify**

- `create wccp [name]`
- `modify wccp [name]`
  - options:
    - `cache-timeout [integer]`
    - `description [string]`
    - `services [add | delete | replace-all-with]`
      - `[object identifier]`
        - options:
          - `hash-fields [dest-ip | dest-port | src-ip | src-port | none]`
          - `password [string | none]`
          - `port-type [none | dest | source]`
          - `ports [integer]`
          - `priority [integer]`
          - `protocol [tcp | udp]`
          - `redirection-method [gre | 12]`
          - `return-method [gre | 12]`
          - `routers [add | delete | modify | replace-all-with]`
            - `[ip address ...]`
          - `traffic-assign [hash | mask]`
          - `tunnel-local-addresses [ip address]`
          - `tunnel-remote-addresses [add | delete | modify | replace-all-with]`
            - `[ip address ...]`
          - `weight [integer]`
    - `edit wccp [ [name] | [glob] | [regex] ] ... ]`
      - options:
        - `all-properties`
        - `non-default-properties`
Display

list wccp
list wccp [ [ [name] | [glob] | [regex] ] ... ]
show running-config wccp
show running-config wccp [ [ [name] | [glob] | [regex] ] ... ]

options:
  all-properties
  non-default-properties
  one-line

Delete

delete wccp [name]

Description

You can use the wccp component to create and modify WCCPv2 service groups. WCCPv2 is a content-routing protocol developed by Cisco Systems, Inc., which provides a mechanism to redirect traffic flows in real time. A WCCP service in this context is a set of redirection criteria and processing instructions that the BIG-IP system applies to any traffic that a router in the service group redirects to the BIG-IP system.

Examples

Displays the services and their attributes in the service group named service-wccp:

list wccp service-wccp all-properties

Changes the cache-timeout setting to 40 for the service group named server-wccp:

modify server-wccp cache-timeout 40

Changes the weight setting to 60 for the service identified as 77 in the service group named server-wccp:

modify server-wccp services modify { 77 {weight 60} }

Options

You can use these options with the wccp component:

- **cache-timeout**
  Specifies the frequency of control messages between the system and the router. The range is from 1 to 60 seconds. The default value is 60.

- **description**
  User-defined description.
◆ **glob**
  Displays the items that match the glob expression. For a description of glob expression syntax, see the glob man page.

◆ **name**
  Specifies a unique name for the component. This option is required for the commands create, delete, and modify.

◆ **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. For a description of regular expression syntax, see the regex man page.

◆ **services**
  Specifies the service group identifier, a number between 51 and 255, that matches a service ID configured on the router.

Adds, deletes, or replaces a set of services. You can configure the following options for a service:

  • **hash-fields**
    Specifies to the router the traffic attributes to use to determine which BIG-IP system it should forward traffic to for load balancing: destination IP address (dest-ip), destination port (dest-port), source IP address (src-ip), and/or source port (src-port).

  • **object identifier**
    Specifies the service group identifier, a number between 51 and 255, that matches a service ID configured on the router.

  • **password**
    Specifies the password for MD5 authentication or none.

  • **port-type**
    Specifies whether the WCCP interception of traffic is based on the destination port (dest) or source port (source), or is not specified (none). The default value is none.

  • **ports**
    Specifies one or more ports (up to 8) on which traffic is redirected.

  • **priority**
    Specifies the precedence of the service group relative to the other service groups. The range is from 1 to 255. The default value is 100.

  • **protocol**
    Specifies the protocol of the traffic to be redirected: TCP (tcp) or (udp). The default value is tcp.

  • **redirection**
    Specifies the method the router uses to redirect traffic: GRE (gre) or L2 (l2). The default value is gre.

  • **return**
    Specifies the method used to return passthrough traffic to the router: GRE (gre) or L2 (l2). The default value is gre.

  • **routers**
    Specifies the IP addresses of the WCCP-enabled routers that redirect traffic.
• **traffic-assign**
  Specifies whether load balancing is achieved by a hash algorithm (hash) or a mask (mask). If you specify hash, specify one or more attributes using the option hash-fields.

• **tunnel-local-addresses**
  Specifies an IP address on the BIG-IP system to which the WCCP-enabled routers should redirect traffic. Specify a self IP address of an external VLAN on the BIG-IP system.

• **tunnel-remote-addresses**
  Specifies the Router Identifier IP address of the router that redirects traffic.

• **weight**
  Specifies the relative importance of this traffic in a load-balancing environment. The range is from 1 to 100. The default value is 50.

**See also**

create, delete, edit, glob, list, modify, regex, show, tmsh
net ipsec Module Components

- Introducing the net ipsec module
- Alphabetical list of components
Introducing the net ipsec module

You can use the `tmsh` components that reside within the `net ipsec` module to configure IP security for the BIG-IP® system. For more information about the `tmsh` hierarchical structure, see Chapter 2, *Understanding and Using the Traffic Management Shell*.

Alphabetical list of components

The remainder of this chapter lists the `tmsh` components that are available in the `net ipsec` module.
ike-daemon

Configures the Internet Key Exchange (ISAKMP) daemon.

Module

net ipsec

Syntax

Configure the \texttt{ike-daemon} component within the \texttt{net ipsec} module using the following syntax.

Create/Modify

\texttt{modify ike-daemon}

\texttt{options:}

- \texttt{description [string]}
- \texttt{isakmp-natt-port [port number]}
- \texttt{isakmp-port [port number]}
- \texttt{log-level [error|warning|notify|info|debug|debug2]}
- \texttt{natt-keep-alive [seconds]}

Display

\texttt{list}

\texttt{list ike-daemon}

\texttt{show running-config ike-daemon}

\texttt{options:}

- \texttt{all-properties}
- \texttt{non-default-properties}
- \texttt{one-line}

Description

You can use the \texttt{ike-daemon} component to configure global settings for the IKE agent.

Examples

Sets the ISAKMP port to 500:

\texttt{modify ike-daemon isakmp-port 500}
Options

You can use these options with the **ike-daemon** component:

- **description**
  User-defined description.

- **isakmp-natt-port**
  Specifies the port that the IKE daemon uses to accept ISAKMP messages when NAT-Traversal is detected. This is also the port number used to accept UDP-encapsulated ESP traffic for NAT-Traversal. Only port **4500** is currently supported.

- **isakmp-port**
  Specifies the port that the IKE daemon uses to accept ISAKMP messages. Only port **500** is currently supported.

- **log-level**
  Specifies the logging level of the IKE daemon. The log file is located at `/var/log/racoon.log`.

- **natt-keep-alive**
  Specifies the interval between sending NAT-Traversal keep-alive packets. The default value is **20** seconds. Set to **0** to disable keep-alive packets.

See also

- list, net ipsec ike-peer, tmsh
ike-peer

Configures one or more IKE peers for IPsec.

Module

net ipsec

Syntax

Configure the ike-peer component within the net ipsec module using the following syntax.

Create/Modify

create ike-peer [string]
modify ike-peer [string]

options:

cert-file [SSL certificate file]
crl-file [SSL CRL file]
description [string]
dpd-delay [integer]
generate-policy [off | on | unique ]
lifetime [minutes]
mode [main | aggressive]
my-cert-file [SSL certificate file]
my-cert-key-file [SSL certificate key file]
my-id-type [address | asn1dn | fqdn | keyid-tag | user-fqdn]
my-id-value [string]
nat-traversal [on | off | force]
passive [true | false]
peers-cert-file [SSL certificate file]
peers-cert-type [certfile | none]
peers-id-type [address | asn1dn | fqdn | keyid-tag | user-fqdn]
peers-id-value [string]
phase1-auth-method [pre-shared-key | rsa-signature]
phase1-encrypt-algorithm [3des | aes | blowfish | camellia | cast128 | des]
phase1-hash-algorithm [md5 | sha1 | sha256 | sha384 | sha512]
phase1-perfect-forward-secrecy [modp1024 | modp1536 | modp2048 | modp3072 | modp4096 |
modp6144 | modp768 | modp8192]
preshared-key [string]
proxy-support [disabled | enabled]
remote-address [ip address]
state [disabled | enabled]
verify-cert [true | false]

Display

list ike-peer
show running-config ike-peer
  options:
    all-properties
    non-default-properties
    one-line
show ike-peer
show ike-peer [name]

Delete

delete ike-peer [string]

Description

You can use the ike-peer component to modify the IKE phase 1 parameters for each remote IKE peer. The setting in the default anonymous ike-peer will apply to any peer that does not match a more specific ike-peer directive.

Examples

Creates an ike-peer named SanJose that has the IP address of 1.2.3.4 using preshared key as the authentication method:

create ike-peer SanJose { remote-address 1.2.3.4 preshared-key abc phase1-auth-method pre-shared-key}

Options

You can use these options with the gre component:

- ca-cert-file
  Specifies the file name of the root certificate authority.

- crl-file
  Specifies the file name of the Certificate Revocation List.

- description
  User-defined description.

- dpd-delay
  This option activates Dead Peer Detection (DPD) and sets the time (in seconds) allowed between two proof of liveness requests. The default value is 3. When the value is set to 0, it means to disable DPD monitoring, but still negotiate DPD support.
◆ **generate_policy**
This directive is for the responder. To use it, set `passive` to `true`, so the IKE peer is only a responder. If the responder does not have any policy in the Security Policy Database (SPD) during phase 2 negotiation, and the directive is set to `on`, then the `raccoon` daemon chooses the first proposal in the Security Association (SA) payload from the initiator, and generates policy entries from the proposal. It is useful to negotiate with clients whose IP address is allocated dynamically. If an inappropriate policy is installed into the responder’s SPD by the initiator, other communications might fail due to a policy mismatch between the initiator and the responder. The initiator ignores this directive. The default value is `off`.  

◆ **lifetime**
Specifies the lifetime of the IKE SA that will be proposed in the phase 1 negotiations.  

◆ **mode**
Specifies the exchange mode for phase 1 when `raccoon` is the initiator, or the acceptable exchange mode when `raccoon` is the responder.  

◆ **my-cert-file**
Specifies the name of `ssl-cert` object for the certificate file.  

◆ **my-cert-key-file**
Specifies the name of `ssl-key` object for the certificate key file.  

◆ **my-id-type**
Specifies the identifier type sent to the remote host to use in the phase 1 negotiation.  

◆ **my-id-value**
Specifies the identifier value sent to the remote host to use in the phase 1 negotiation.  

◆ **nat-traversal**
Enables use of the NAT-Traversal IPsec extension (NAT-T). NAT-T allows one or both peers to reside behind a NAT gateway (that is, performing address- or port-translation). The presence of NAT gateways along the path is discovered during the phase 1 handshake, and if found, NAT-T is negotiated. When NAT-T is in charge, all ESP and AH packets of a given connection are encapsulated into UDP datagrams (port 4500, by default). The options are:  
  - **force**
    NAT-T is used regardless of whether NAT is detected between the peers.  
  - **off**
    NAT-T is not proposed/accepted. This is the default.  
  - **on**
    NAT-T is used when a NAT gateway is detected between the peers.  

◆ **passive**
Specify `true` if you do not want to be the initiator of the IKE negotiation with this `ike-peer`.  

---

36 - 6
- **peers-cert-file**
  Specifies, if `peers-cert-file` is defined, that the isakmp daemon ignores the CERT payload from the peer and use this certificate as the peer's certificate.

- **peers-cert-type**
  Specifies that `certfile` is the only `peers-cert-type` supported.

- **peers-id-type**
  Specifies that `address`, `fqdn`, `asn1dn`, `user-fqdn`, or `keyid-tag` can be used as `peers-id-type`.

- **peers-id-value**
  Specifies the peer's identifier to be received. If it is not defined, then the IKE agent will not verify the peer's identifier in the ID payload transmitted from the peer. The usage of `peers-id-type` and `peers-id-value` is the same as `my-id-type` and `my-id-value` except that the individual component values of an `asn1dn` identifier can specified as `*` to match any value (for example, "C=XX, O=MyOrg, OU=*, CN=Mine").

- **phase1-auth-method**
  Defines the authentication method used for the phase 1 negotiation. Possible values are: `pre-shared-key` and `rsa-signature`. Use `rsa-signature` if using X.509 certificates.

- **phase1-encrypt-algorithm**
  Specifies the encryption algorithm used for the ISAKMP phase 1 negotiation. This directive must be defined. Possible value is one of following: `des`, `3des`, `blowfish`, `cast128`, `aes`, or `camellia` for Oakley.

- **phase1-hash-algorithm**
  Defines the hash algorithm used for the ISAKMP phase 1 negotiation. This directive must be defined. The algorithm should be one of following: `md5`, `sha1`, `sha256`, `sha384`, or `sha512` for Oakley.

- **phase1-perfect-forward-secrecy**
  Defines the group used for the Diffie-Hellman exponentiations to provide perfect forward secrecy. This directive must be defined. The group is one of following: `modp768`, `modp1024`, `modp1536`, `modp2048`, `modp3072`, `modp4096`, `modp6144`, or `modp8192`.

- **preshared-key**
  Specifies the preshared key for ISAKMP SAs. This field is valid only when `phase1-auth-method` is `pre-shared-key`.

- **proxy-support**
  If this value is `enabled`, both values of the ID payloads in the phase 2 exchange are used as the addresses of the IPsec security association endpoints. The default is `enabled`.

- **remote-address**
  Specifies the IP address of the IKE remote node.

- **state**
  Enables or disables this IKE remote node.
verify-cert
Specifies that by default, the identifier sent by the remote host (as specified in its my_identifier statement) is compared with the credentials in the certificate used to authenticate the remote host as follows: Type
asn1dn: The entire certificate subject name is compared with the identifier; that is, "C=XX, O=YY," and so on. Type address, fqdn, or user_fqdn: The certificate's subjectAltName is compared with the identifier. If the two do not match, the negotiation fails. If you do not want to verify the identifier using the peer's certificate, set this to false.

See also
create, delete, list, tmsh
ipsec-policy

Configures an IP over IP (IPIP) profile.

Module

net ipsec

Syntax

Configure the ipsec-policy component within the net ipsec module using the following syntax.

Create/Modify

create ipsec-policy [name]
modify ipsec-policy [name]

options:
  description [string]
  ike-phase2-auth-algorithm [aes-gcm128 | aes-gcm192 | aes-gcm256 | aes-gmac128 | aes-gmac192 | aes-gmac256 | sha1]
  ike-phase2-lifetime [integer]
  ike-phase2-perfect-forward-secrecy [modp1024 | modp1536 | modp2048 | modp3072 | modp4096 | modp6144 | modp768 | modp8192]
  mode [transport | tunnel | isession]
  protocol [esp]
  tunnel-local-address [ip address]
  tunnel-remote-address [ip address]

Display

list ipsec-policy
list ipsec-policy
list ipsec-policy [ [ [name] | [glob] | [regex] ] ... ]
show running-config ipsec-policy
show running-config ipsec-policy [ [ [name] | [glob] | [regex] ] ... ]

options:
  all-properties
  non-default-properties
  partition

show ipsec-policy
show ipsec-policy [name]
Delete

show ipsec-policy [name]

Description

An ipsec-policy indicates the IPsec rule and action to be applied to the packets matched by the traffic-selector associated with this ipsec-policy.

Examples

Creates an IPsec policy tunnel_policy_sjc_sea for traffic in a tunnel between local IP address 1.1.1.1 and a remote IP address 2.2.2.2:

<create ipsec ipsec-policy tunnel_policy_sjc_sea { description "ipsec policy for the sjc-sea ipsec tunnel" mode tunnel tunnel-local-address 1.1.1.1 tunnel-remote-address 2.2.2.2 }>

Deletes the IPsec policy tunnel_policy_sjc_sea:

delete ipsec ipsec-policy tunnel_policy_sjc_sea

Options

You can use these options with the ipsec-policy component:

- **description**
  User-defined description.

- **ike-phase2-auth-algorithm**
  Specifies a payload authentication algorithm for ESP. This attribute is only valid when IKE is used to negotiate Security Associations. The possible options are: aes-gcm128, aes-gcm192, aes-gcm256, aes-gmac128, aes-gmac192, aes-gmac256, and sha1. The default value is aes-gcm128.

  Note: Because aes-gcm and aes-gmac are authenticated encryption algorithms, when the ike-phase2-auth-algorithm is set to aes-gcm or aes-gmac, the ike-phase2-encrypt-algorithm has to be set to the identical algorithm with the same key length. The algorithm sha1 can be used only with an encryption algorithm that is NOT an authenticated encryption algorithm.

- **ike-phase2-lifetime**
  Specifies the lifetime duration for the dynamically-negotiated security associations (SA). This attribute is only valid when IKE is used to negotiate security associations.

- **ike-phase2-encrypt-algorithm**
  Specifies an encryption algorithm for ESP. This attribute is only valid when IKE is used to negotiate security associations. The default value is aes-gcm128.
Note: Because `aes-gcm` and `aes-gmac` are authenticated encryption algorithms, when the `ike-phase2-encrypt-algorithm` is set to one of these algorithms, the `ike-phase2-auth-algorithm` must be set to the identical algorithm with the same key length.

- **ike-phase2-perfect-forward-secrecy**
  Defines the group of Diffie-Hellman exponentiations. This attribute is only valid when IKE is used to negotiate Security Associations.

- **mode**
  Specifies a security protocol mode for use. The options are:
  - **transport**
    IPsec transport mode is used.
  - **tunnel**
    IPsec tunnel mode is used.
  - **isession**
    A special tunnel mode `ipsec-policy` that is applicable only to the local and remote endpoints of a WOM iSession connection.

- **protocol**
  Specifies the IPsec protocol: Encapsulating Security Payload (ESP) or Authentication Header (AH).

- **tunnel-local-address**
  Specifies the IP address of the local IPsec tunnel endpoint. This option is valid only when mode is `tunnel`.

- **tunnel-remote-address**
  Specifies the IP address of the remote IPsec tunnel endpoint. This option is valid only when mode is `tunnel`.

See also

- `list`, `modify`, `net ipsec traffic-selector`, `net ipsec manual-security-association`, `tmsh`
manual-security-association

Configures the IPsec manual-security-association.

Module

net ipsec

Syntax

Configure the manual-security-association component within the net ipsec module using the following syntax.

Create/Modify

create manual-security-association
modify manual-security-association
options:
  description [string]
  auth-algorithm [sha1]
  auth-key [key]
  destination-address [ip address]
  encrypt-algorithm [3des|aes128|aes192|aes256|null]
  ipsec-policy [name]
  protocol [esp]
  source-address [ip address]
  spi [number]

Display

list manual-security-association
show manual-security-association
show running-config manual-security-association
options:
  app-service
  all-properties
  non-default-properties
  one-line

Delete

delete manual-security-association [name]
Description

Manually configures Security Association Database (SAD) entries. Because each SA provides data protection only for unidirectional traffic, you must configure a manual-security-association for traffic in each direction to establish a bidirectional IPsec tunnel.

Examples

Creates a manual-security-association object named msa_on_dut2_transport_in to use IPsec to protect traffic from 2.2.2.2 to 7.7.7.7 with the authentication key test and the encryption key test. The ipsec-policy object named transport_policy_on_dut2 is associated with this manually configured security association:

```
create ipsec manual-security-association msa_on_dut2_transport_in { auth-key test description "manual security association on dut2 for dut1 - transport" destination-address 7.7.7.7 encrypt-key test ipsec-policy transport_policy_on_dut2 source-address 2.2.2.2 spi 1025 }
```

Options

You can use these options with the manual-security-association component:

- **app-service**
  Displays the application service to which the object belongs

- **auth-algorithm**
  Specifies an authentication algorithm.

- **auth-key**
  Specifies the key for the authentication algorithm.

- **description**
  User-defined description.

- **destination-address**
  Specifies the destination of the security association.

- **encrypt-algorithm**
  Specifies an encryption algorithm.

- **ipsec-policy**
  Specifies the ipsec-policy associated with this manual-security-association.

- **protocol**
  Specifies the IPsec protocol: Encapsulating Security Payload (ESP) or Authentication Header (AH).

- **source-address**
  Specifies the source address of the security association.
spi
Specifies the Security Parameters Index. If this is the Security Association (SA) for the outbound traffic, make sure it matches the SPI of the inbound SA configured on the remote site and vice versa. SPI values between 0 and 255 are reserved for the future use by IANA, and cannot be used.

See also

list, modify, net ipsec ipsec-policy, tmsh
traffic-selector

Configures a traffic selector for IPsec.

Module

net ipsec

Syntax

Configure the traffic-selector component within the net ipsec module using the following syntax.

Create/Modify

create traffic-selector [name]
modify traffic-selector [name]

options:
  action [protect]
  description [string]
  destination-address [ip address/netmask]
  direction [both | in | out]
  ipsec-policy [name]
  source-address [ip address/netmask]

Display

list
list traffic-selector

Delete

delete traffic-selector [name]

Description

You can use the traffic-selector component to specify which incoming traffic you want the system to protect with IPsec.
Examples

Creates a **traffic-selector** named sjc2sea, which has the IP address of 10.10.10.0/24 using **ipsec-policy** named **my_policy**:

```
create traffic-selector sjc2sea { source-address 10.10.10.0/24
destination address 20.20.20.0/24 direction both ipsec-policy
my_policy}
```

Options

You can use these options with the **traffic-selector** component:

- **description**
  User-defined description.

- **direction**
  Specifies the direction of traffic to be protected with IPsec. If the **direction** is **both**, use **source-address** and **destination-address** with respect to the outbound direction. The default value is **both**.

- **ipsec-policy**
  Specifies the name of the IPsec policy to be enforced on the matched traffic.

- **source-address**
  Specifies the source IP address of the traffic to be matched.

See also

- list, net ipsec ipsec-policy, tmsh
net rate-shaping Module Components

- Introducing the net rate-shaping module
- Alphabetical list of components
Introducing the net rate-shaping module

You can use the `tmsh` components that reside within the **net rate-shaping** module to configure rate shaping for the network. For more information about the `tmsh` hierarchical structure, see Chapter 2, *Understanding and Using the Traffic Management Shell*.

Alphabetical list of components

The remainder of this chapter lists the `tmsh` components that are available in the **net rate-shaping** module.
class

Configures a rate class.

Module

net rate-shaping

Syntax

Configure the class component within the net rate-shaping module using the following syntax.

Create/Modify

create class [name]
modify class [name]

options:
  ceiling [integer]
  ceiling-percentage [integer]
  description [string]
  direction [any | to-client | to-server]
  drop-policy [ [custom drop policy name] | fred | red | tail]
  max-burst [integer]
  parent [class name]
  queue [ [custom queue name] | pfifo | sfq]
  rate [integer]
  rate-percentage [integer]
  shaping-policy [ [custom shaping policy name] | none]

edit class [ [ [name] | [glob] | [regex] ] ... ]

options:
  all-properties
  non-default-properties

Display

list class
list class [ [ [name] | [glob] | [regex] ] ... ]

show running-config class
show running-config class [ [ [name] | [glob] | [regex] ] ... ]

options:
  all-properties
  non-default-properties
  one-line
partition

show class

show class [ [ name ] | [ glob ] | [ regex ] ] ...

options:

   current-module

   ( default | exa | gig | kil | meg | peta | raw | tera | yotta | zetta )

Delete

   delete class [ name ]

Description

You can use the class component to create a rate class. A rate class lets you specify shaping properties for a specific type of traffic, such as Layer 3 traffic that specifies a certain source, destination, or service. Specifically, a rate class defines the number of bits per second that the system accepts per flow and the number of packets in a queue.

You configure rate shaping by creating a class and then assigning the class to a packet filter, a virtual server, or from within an iRule. When you configure a class, you can associate another class with the class you are configuring using the parent option.

You can also associate drop policies, queues, and shaping policies with a class using the drop-policy, queue, and shaping policy options, respectively, of the class component. You can associate pre-configured drop policies and queues with the class, or you can create custom drop policies, queues, and shaping policies, and then associate them with the class. For more information about creating these components, see drop-policy, on page 37-7, queue, on page 37-11, and shaping-policy, on page 37-14.

◆ Note

If you specify a value for the shaping-policy option of the class component, the system automatically changes the ceiling-percentage, drop-policy, max-burst, queue, and rate-percentage options of the class to match the values in the specified shaping policy.

Examples

Creates a class named my_class with a rate of 10:

create class my_class rate 10

Displays all of the properties of all of the classes:

list class all-properties
Options

You can use these options with the `class` component:

- **ceiling**
  Specifies how far, beyond the value specified for the `rate` option, that traffic can flow when bursting. This number sets an absolute limit. No traffic can exceed this rate. The rate class might limit traffic throughput to the value of the `rate` option when there is high contention among siblings of a parent-child class hierarchy. The default value is the value of the `rate` option. The minimum value is **296 bps**.

- **ceiling-percentage**
  Specifies the ceiling of the rate class as a percentage of the ceiling of the associated parent class. This option applies only to rate classes with an associated parent rate class. The default value is **0 (zero)**, which indicates that the class uses the value of the `ceiling` option.

- **description**
  User-defined description.

- **direction**
  Specifies the direction of traffic to which the class is applied. The default value is **any**.

- **drop-policy**
  Specifies the name of a drop policy. You can use one of the pre-configured drop policies, or you can create a customized drop policy using the `drop-policy` component.
  The default value is **tail**, which is the simplest pre-configured drop policy. The pre-configured drop policies are:
  - **fred**
    Specifies that the system uses flow-based random early detection (FRED) to decide whether to drop packets based on the aggressiveness of each flow.
  - **red**
    Specifies that the system uses random early detection (RED) to determine whether to drop packets to maintain the average queue length within the specified range.
  - **tail**
    Specifies that the system drops all incoming packets when the queue is full.

- **glob**
  Displays the items that match the `glob` expression. For a description of `glob` expression syntax, see the `glob` man page.

- **max-burst**
  Specifies the maximum number of bytes that traffic can burst beyond the value of the `rate` option. The traffic cannot burst higher than the value of the `ceiling` option. The default value is **0 (zero)**.

- **name**
  Specifies a unique name for the component. This option is required for the commands `create`, `delete`, and `modify`.
◆ **parent**
Associates another class with this class. The class you are configuring (which when you configure a parent class for it becomes a child class) can borrow bandwidth from the parent class. The parent class can use any of the unused bandwidth of the child class. Borrowing bandwidth affects the value of the `ceiling`, `queue`, and `rate` options of both classes. The default value is `none`.

◆ **queue**
Specifies the queuing method. The pre-configured options are:

- **pfifo**
The Priority FIFO queuing method queues all traffic under a set of five sub-queues based on the Type of Service (TOS) field of the traffic. Four of the sub-queues correspond to the four possible TOS values (minimum delay, maximum throughput, maximum reliability, and minimum cost). The fifth sub-queue represents traffic with no TOS value. The Priority FIFO method processes these five sub-queues in a way that preserves the meaning of the TOS value as much as possible. For example, a packet with the TOS value of minimum cost might yield dequeueing to a packet with the TOS value of minimum delay.

- **sfq**
Stochastic Fair Queuing (SFQ) is a queuing method that further queues packets under a set of many FIFO sub-queues. Selection of a specific sub-queue is based on a hash of the flow address information. SFQ dequeues packets from the set of sub-queues in a Round Robin fashion. The overall effect is that fairness of dequeuing is achieved, because packets from one flow cannot occupy the queues at the exclusion of those of another flow. If you assign a shaping policy to the class, then the queuing discipline of the class becomes that specified in the shaping policy. If you do not assign a shaping policy to the class, the default queue is `sfq`.

◆ **rate**
Specifies the guaranteed throughput rate of the traffic handled by this rate class. You can configure the rate in bits per second (bps), kilobits per second (Kbps), megabits per second (Mbps), or gigabits per second (Gbps).

◆ **rate-percentage**
Specifies the rate of the rate class as a percentage of the ceiling of the associated parent class. This option applies only to rate classes with an associated parent rate class. The default value is 0 (zero), which specifies that the system uses the value of the `rate` option.

◆ **regex**
Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. For a description of regular expression syntax, see the `regex` man page.
shaping-policy
Specifies the name of a shaping policy. The default value is none.
The system automatically changes the ceiling-percentage, drop-policy,
max-burst, queue, and rate-percentage options of this class to match
the values in the specified shaping policy.

See also

create, delete, edit, glob, list, modify, net rate-shaping drop-policy, net
rate-shaping queue, net rate-shaping shaping-policy, regex, show, tmsh
drop-policy

Configures a custom drop policy for use in rate shaping.

Module

net rate-shaping

Syntax

Configure the drop-policy component within the net rate-shaping module using the following syntax.

Create/Modify

create drop-policy [name]
modify drop-policy [name]
  options:
    average-packet-size [integer]
    description [string]
    fred-max-active [integer]
    fred-max-drop [integer]
    fred-min-drop [integer]
    inverse-weight [integer]
    max-probability [integer]
    max-threshold [integer]
    min-threshold [integer]
    red-hard-limit [integer]
    type [fred | red | tail]
edit drop-policy [ [ [name] | [glob] | [regex] ] ... ]
  options:
    all-properties
    non-default-properties

Display

list drop-policy
list drop-policy [ [ [name] | [glob] | [regex] ] ... ]
show running-config drop-policy
show running-config drop-policy [ [ [name] | [glob] | [regex] ] ... ]
  options:
    all-properties
    non-default-properties
    one-line
Delete

```
delete drop-policy [name]
```

Description

A drop policy tells the system when and how to drop packets when the traffic handling queue is full, if required. The system comes with three pre-configured drop policies: fred, red, and tail.

You can use the drop-policy component to create a custom drop policy, and then associate it with a class using the drop-policy option of the class component. For more information, see class, on page 37-2.

You can also associate a custom drop policy with a shaping policy using the drop-policy option of the shaping-policy component. For more information, see shaping-policy, on page 37-14.

Examples

Creates a custom drop policy named my_dp:

```
create drop-policy my_dp
```

Displays all of the properties of all of the drop policies:

```
list drop-policy all-properties
```

Options

You can use these options with the drop-policy component:

- **average-packet-size**
  Specifies the average MTU (maximum transmission unit) size in the range of 0 to 10000 bytes. The default value is 0 (zero).

- **description**
  User-defined description.

- **fred-max-active**
  Specifies the maximum number of flows that can be active for each queue. The range is 0 to 10000. The default value is 0 (zero), which disables active flow limitation.

- **fred-max-drop**
  Specifies a hard drop limit in the range of 0 to 400. The default value is 0 (zero). Setting this to a small value does not change the hard drop limit, but a higher number increases the limit.

- **fred-min-drop**
  Specifies a hard no-drop limit in the range of 0 to 100. The default value is 0 (zero). Setting this to a large value prevents packets from being dropped.
◆ glob
Displays the items that match the glob expression. For a description of glob expression syntax, see the glob man page.

◆ inverse-weight
Specifies the weight used to calculate the average queue length. Valid values are 0, 64, 128, 256, 512, and 1024. The default value is 0 (zero).

◆ max-probability
Specifies the maximum percentage probability in the range of 0 to 100 according to which packets are dropped when the average queue length is between the minimum and maximum thresholds. The default value is 0 (zero).

◆ max-threshold
Specifies the maximum queue length. The default value is 0 (zero).

◆ min-threshold
Specifies the minimum queue length. The default value is 0 (zero).

◆ name
Specifies a unique name for the component. This option is required for the commands create, delete, and modify.

◆ red-hard-limit
Specifies the maximum queue size in bytes. Additional packets are dropped. The default value is 0 (zero).
This option applies only when the value of the type option is red.

◆ regex
Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. For a description of regular expression syntax, see the regex man page.

◆ type
Specifies the type of drop policy. The default value is red.
The options are:
  • fred
    Specifies that the system uses flow-based random early detection (FRED) to decide whether to drop packets based on the aggressiveness of each flow.
  • red
    Specifies that the system uses random early detection (RED) to determine whether to drop packets to maintain the average queue length within the specified range.
  • tail
    Specifies that the system drops all incoming packets when the queue is full. This is the simplest drop policy.

Note: Although you could create a drop policy based on tail, that is already the default value of the drop-policy option in both the shaping-policy and class components.
See also

create, delete, edit, glob, list, modify, net rate-shaping class, net rate-shaping queue, net rate-shaping shaping-policy, regex, show, tmsh
queue

Configures a custom queuing method.

Module

net rate-shaping

Syntax

Configure the queue component within the net rate-shaping module using the following syntax.

Create/Modify

create queue [pfifo | sfq]
modify queue [all | pfifo | sfq]
   options:
      description [string]
      pfifo-max-size [integer]
      pfifo-min-size [integer]
      sfq-bucket-count [integer]
      sfq-bucket-size [integer]
      sfq-perturbation [integer]
      type [pfifo | sfq]
edit queue [ [ [name] | [glob] | [regex] ] ... ]
   options:
      all-properties
      non-default-properties
      one-line

Display

list queue
list queue [ [ all | pfifo | sfq ] | [glob] | [regex] ] ... ]
show running-config queue
show running-config queue [ [ all | pfifo | sfq ] | [glob] | [regex] ] ... ]
   options:
      all-properties
      non-default-properties

Delete

delete queue [all | pfifo | sfq]
Chapter 37

Description

You can use the `queue` component to configure a custom queuing method.

Examples

Creates a `pfifo` type queue name `my_q`:

```
create queue my_q type pfifo
```

Displays all of the properties of all of the queues:

```
list queue all-properties
```

Options

You can use these options with the `queue` component:

- **description**
  User-defined description.

- **glob**
  Displays the items that match the `glob` expression. For a description of `glob` expression syntax, see the `glob` man page.

- **name**
  Specifies a unique name for the component. This option is required for the commands `create`, `delete`, and `modify`.

- **pfifo-max-size**
  Specifies the size, in bytes, of the largest queue for the `pfifo` type only. The default value is 0 (zero).

- **pfifo-min-size**
  Specifies the size, in bytes, of the smallest queue for the `pfifo` type only. The default value is 0 (zero).

- **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. For a description of regular expression syntax, see the `regex` man page.

- **sfq-bucket-count**
  Specifies the number of buckets into which the queue is divided when you are configuring the `sfq` type. Valid values are 0, 16, 32, 64, 128, 256, 512, and 1024. The default value is 0 (zero).

- **sfq-bucket-size**
  Specifies the bucket size, in bytes, for the `sfq` type. The default value is 0 (zero).

- **sfq-perturbation**
  Specifies the interval in seconds at which the system reconfigures the SFQ hash function. The default value is 0 (zero).
net rate-shaping Module Components

◆ type
   Specifies the queuing method this custom queue uses.
   The options are:
   - pfifo
     The Priority FIFO queuing method queues all traffic under a set of
     five sub-queues based on the Type of Service (TOS) field of the traffic. Four of the sub-queues correspond to the four possible TOS values (minimum delay, maximum throughput, maximum reliability, and minimum cost). The fifth sub-queue represents traffic with no TOS value. The Priority FIFO method processes these five sub-queues in a way that preserves the meaning of the TOS value as much as possible. For example, a packet with the TOS value of minimum cost might yield dequeuing to a packet with the TOS value of minimum delay.
   - sfq
     Stochastic Fair Queuing (SFQ) is a queuing method that further queues packets under a set of many FIFO sub-queues. Selection of a specific sub-queue is based on a hash of the flow address information. SFQ dequeues packets from the set of sub-queues in a Round Robin fashion. The overall effect is that fairness of dequeuing is achieved, because packets from one flow cannot occupy the queues at the exclusion of those of another flow.

See also

create, delete, edit, glob, list, modify, net rate-shaping class, net rate-shaping drop-policy, net rate-shaping shaping-policy, regex, show, tmsh
Chapter 37

shaping-policy

Configures a custom rate shaping policy for traffic flow.

Module

net rate-shaping

Syntax

Configure the shaping-policy component within the net rate-shaping module using the following syntax.

Create/Modify

create shaping-policy [name]
modify shaping-policy [name]
  options:
    ceiling-percentage [integer]
    description [string]
    drop-policy [ [name] | none]
    max-burst [integer]
    queue [ [name] | none]
    rate-percentage [integer]
edit shaping-policy [ [ [name] | [glob] | [regex] ] ... ]
  options:
    all-properties
    non-default-properties
    one-line

Display

list shaping-policy
list shaping-policy [name]
show running-config shaping-policy
show running-config shaping-policy [name]
  options:
    all-properties
    non-default-properties

Delete

delete shaping-policy [name]
Description

You can use the shaping-policy component to create a custom rate shaping policy to handle traffic flow, and then associate the shaping policy with a class.

**Note**

If you specify a value for the shaping-policy option of a class, the system automatically changes the ceiling-percentage, drop-policy, max-burst, queue, and rate-percentage options of that class to match the values in the shaping policy.

Examples

Creates a shaping policy named my_sp:

```
create shaping-policy my_sp
```

Displays all of the properties of all of the shaping policies:

```
list shaping-policy all-properties
```

Options

You can use these options with the shaping-policy component:

- **ceiling-percentage**
  Specifies the percentage of the value of the ceiling option specified for the parent associated with the class component to which this shaping policy is associated. The default value is 0 (zero).

- **description**
  User-defined description.

- **drop-policy**
  Specifies a drop policy for this traffic flow. The default value is tail. You can use one of the pre-configured drop policies, or you can create a customized drop policy using the drop-policy component. For more information, see drop-policy, on page 37-7.

  The available pre-configured drop policies are:

  - **fred**
    Specifies that the system uses flow-based random early detection (FRED) to decide whether to drop packets based on the aggressiveness of each flow.

  - **red**
    Specifies that the system uses random early detection (RED) to determine whether to drop packets to maintain the average queue length within the specified range.

  - **tail**
    Specifies that the system drops all incoming packets when the queue is full. This is the simplest drop policy.
◆ **glob**
Displays the items that match the glo\_b expression. For a description of glo\_b expression syntax, see the glo\_b man page.

◆ **max-burst**
Specifies the maximum number of bytes that traffic can burst beyond the value of the rate option of the class component to which this shaping policy is associated. The default value is 0 (zero).

◆ **name**
Specifies a unique name for the component. This option is required for the commands create, delete, and modify.

◆ **queue**
Specifies the queuing method for this traffic flow. The default value is none. You can create a customized queuing method using the queue component. The pre-configured queues are:

* **pfifo**
The Priority FIFO queuing method queues all traffic under a set of five sub-queues based on the Type of Service (TOS) field of the traffic. Four of the sub-queues correspond to the four possible TOS values (minimum delay, maximum throughput, maximum reliability, and minimum cost). The fifth sub-queue represents traffic with no TOS value. The Priority FIFO method processes these five sub-queues in a way that preserves the meaning of the TOS value as much as possible. For example, a packet with the TOS value of minimum cost might yield dequeuing to a packet with the TOS value of minimum delay.

* **sfq**
Stochastic Fair Queuing (SFQ) is a queuing method that further queues packets under a set of many FIFO sub-queues. Selection of a specific sub-queue is based on a hash of the flow address information. SFQ dequeues packets from the set of sub-queues in a Round Robin fashion. The overall effect is that fairness of dequeuing is achieved, because packets from one flow cannot occupy the queues at the exclusion of those of another flow.

◆ **rate-percentage**
Specifies the percentage of the value of the rate option of the parent of the class component to which this shaping policy is associated that is available for this traffic flow. The default value is 0 (zero).

◆ **regex**
Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. For a description of regular expression syntax, see the regex man page.

See also

create, delete, edit, glo\_b, list, modify, net rate-shaping class, net rate-shaping drop-policy, net rate-shaping queue, regex, show, tmsh
net tunnels Module Components

- Introducing the net tunnels module
- Alphabetical list of components
Introducing the net tunnels module

You can use the tmsh components that reside within the net tunnels module to configure tunnels for the BIG-IP® system. For more information about the tmsh hierarchical structure, see Chapter 2, Understanding and Using the Traffic Management Shell.

Alphabetical list of components

The remainder of this chapter lists the tmsh components that are available in the net tunnels module.
etherip

Configures an EtherIP tunnel profile.

Module

net tunnels

Syntax

Configure the etherip component within the net tunnels module using the following syntax.

Create/Modify

create etherip [name]
modify etherip [name]
    options:
        defaults-from [name]
        description [string]
edit etherip [ [ [name] | [glob] | [regex] ] ... ]
    options:
        all-properties
        non-default-properties

Display

list etherip
list etherip [ [ [name] | [glob] | [regex] ] ... ]
show running-config etherip
show running-config etherip [ [ [name] | [glob] | [regex] ] ... ]
    options:
        all-properties
        app-service
        non-default-properties
        one-line
        partition

Delete

delete etherip [ all | [name] ]
Description

You can use the `etherip` component to create an EtherIP profile that you associate with a tunnel using the `tunnel` component. This will cause ethernet frames to be sent over the tunnel. For more information about creating a tunnel, see `net tunnel`.

Examples

Creates an EtherIP profile called `my_etherip`:

```
create etherip my_etherip
```

Displays all of the properties of all EtherIP profiles:

```
list etherip all-properties
```

Options

You can use these options with the `etherip` component:

- **app-service**
  Displays the application service to which the object belongs. The default value is `none`.
  
  **Note:** If the `strict-updates` option is enabled on the Application Service that owns the object, you cannot modify or delete the object. Only the Application Service can modify or delete the object.

- **defaults-from**
  Specifies the existing profile from which the system imports settings for the new profile. The default value is `etherip`.

- **description**
  User-defined description.

- **glob**
  Displays the items that match the `glob` expression. For a description of `glob` expression syntax, see the `glob` man page.

- **name**
  Specifies a unique name for the component. This option is required for the commands `create` and `modify`.

- **partition**
  Displays the partition within which this component resides.

- **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (`@[regular expression]`) to indicate that the identifier is a regular expression. For a description of regular expression syntax, see the `regex` man page.
See also

create, delete, edit, glob, list, modify, net tunnels ipip, net tunnels tunnel, net tunnels wccp, regex, show, tmsh
gre

Configures a Generic Router Encapsulation (GRE) profile.

Module

net tunnels

Syntax

Configure the gre component within the net tunnels module using the following syntax.

Create/Modify

create gre [name]
modify gre [name]
  options:
    defaults-from [name]
    description [string]
    rx-csum [disabled | enabled]
    tx-csum [disabled | enabled]
edit gre [ [ [name] | [glob] | [regex] ] ... ]
  options:
    all-properties
    non-default-properties

Display

list gre
list gre [ [ [name] | [glob] | [regex] ] ... ]
show running-config gre
show running-config gre [ [ [name] | [glob] | [regex] ] ... ]
  options:
    all-properties
    app-service
    non-default-properties
    one-line
    partition

Delete

delete gre [all | [name] ]
Chapter 38

Description

You can use the `gre` component to create a GRE profile that you associate with a tunnel using the `tunnel` component. For more information about creating a tunnel, see `tunnel`, on page 38-14.

Examples

Creates a GRE profile named `my_gre`:

```
create gre my_gre
```

Displays all of the properties of all of the GRE profiles:

```
list gre all-properties
```

Options

You can use these options with the `gre` component:

- **app-service**
  Displays the application service to which the object belongs. The default value is `none`.
  
  **Note:** If the `strict-updates` option is enabled on the Application Service that owns the object, you cannot modify or delete the object. Only the Application Service can modify or delete the object.

- **defaults-from**
  Specifies the existing profile from which the system imports settings for the new profile. The default value is `gre`.

- **description**
  User-defined description.

- **glob**
  Displays the items that match the `glob` expression. For a description of `glob` expression syntax, see the `glob` man page.

- **name**
  Specifies a unique name for the component. This option is required for the `create` and `modify` commands.

- **partition**
  Displays the partition within which this component resides.

- **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. For a description of regular expression syntax, see the `regex` man page.

- **rx-csum**
  Specifies whether the system verifies the checksum on received packets. The default value is `disabled`. 
◆ tx-csum
   Specifies whether the system includes a checksum on transmitted packets. The default value is disabled.

See also

create, delete, edit, glob, list, modify, net tunnels ipip, net tunnels tunnel, net tunnels wccp, regex, show, tmsh
ipip

Configures an IP over IP (IPIP) profile.

Module

net tunnels

Syntax

Configure the ipip component within the net tunnels module using the following syntax.

Create/Modify

create ipip [name]
modify ipip [name]
  options:
    defaults-from [name]
    description [string]
    proto [IPv4 | IPv6]
edit ipip [ [ [name] | [glob] | [regex] ] ... ]
  options:
    all-properties
    non-default-properties

Display

list ipip
list ipip [ [ [name] | [glob] | [regex] ] ... ]
show running-config ipip
show running-config ipip [ [ [name] | [glob] | [regex] ] ... ]
  options:
    all-properties
    app-service
    non-default-properties
    one-line
    partition

Delete

delete ipip [all | [name] ]
Description

You can use the `ipip` component to create an IPIP profile that you associate with a tunnel using the `tunnel` component. For more information about creating a tunnel, see `tunnel`, on page 38-14.

Examples

Creates an IPIP profile named `my_ipip`:

```
create ipip my_ipip
```

Displays all of the properties of all of the IPIP profiles:

```
list ipip all-properties
```

Options

You can use these options with the `ipip` component:

- **app-service**
  Displays the application service to which the object belongs. The default value is `none`.
  
  **Note:** If the `strict-updates` option is enabled on the Application Service that owns the object, you cannot modify or delete the object. Only the Application Service can modify or delete the object.

- **defaults-from**
  Specifies the existing profile from which the system imports settings for the new profile. The default value is `ipip`.

- **description**
  User-defined description.

- **glob**
  Displays the items that match the `glob` expression. For a description of `glob` expression syntax, see the `glob` man page.

- **name**
  Specifies a unique name for the component. This option is required for the `create` and `modify` commands.

- **partition**
  Displays the partition within which this component resides.

- **proto**
  Specifies the next header protocol. The default value is `IPv4`.

- **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. For a description of regular expression syntax, see the `regex` man page.
See also

create, delete, edit, glob, list, modify, net tunnels gre, net tunnels tunnel, net tunnels wccp, regex, show, tmsh
PPP

Configures a PPP profile.

Module

net tunnels

Syntax

Configure the ppp component within the net tunnels module using the following syntax.

Create/Modify

create ppp [name]
modify ppp [name]

options:
  defaults-from [ [name] | none]
description [string]
lcp-echo-failure [integer]
lcp-echo-interval [integer]
vj [disabled | enabled]
edit ppp [ [ [name] | [glob] | [regex] ] ... ]

options:
  all-properties
  non-default-properties

Display

list ppp
list ppp [ [ [name] | [glob] | [regex] ] ... ]
show running-config ppp
show running-config ppp [ [ [name] | [glob] | [regex] ] ... ]

options:
  all-properties
  app-service
  non-default-properties
  one-line
  partition

Delete

delete ppp [ all | [name] ]
Description

You can use the `ppp` component to create a ppp profile that you associate with a tunnel using the `tunnel` component. For more information about creating a tunnel see `net tunnel`.

Examples

Creates a PPP profile called `my_ppp`:
```
create ppp my_ppp
```

Displays all the properties of all the PPP profiles:
```
llist ppp all-properties
```

Options

You can use these options with the `ppp` component:

- **app-service**
  Displays the application service to which the object belongs. The default value is `none`.

  *Note: If the `strict-updates` option is enabled on the Application Service that owns the object, you cannot modify or delete the object. Only the Application Service can modify or delete the object.*

- **defaults-from**
  Specifies the existing profile from which the system imports settings for the new profile. The default value is `ppp`.

- **glob**
  Displays the items that match the `glob` expression. For a description of `glob` expression syntax, see the `glob` man page.

- **lcp-echo-failure**
  Specifies the number of consecutive PPP LCP echo messages that must go unanswered for the server to drop PPP connection. For example, if the server sends `number` of consecutive PPP LCP Echo Request messages that go unanswered (by Echo Reply), it will close the PPP connection. The default value is `4`.

- **lcp-echo-interval**
  Specifies the interval, in seconds, between the PPP LCP Echo Request messages that the server sends to the peer (client). The default value is `30`.

- **name**
  Specifies a unique name for the component. This option is required for the commands `create` and `modify`.

- **partition**
  Displays the partition within which this component resides.
- **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. See `help regex` for a description of regular expression syntax.

- **vj**
  Specifies whether the system uses Van Jacobson Header Compression (also known as VJ compression, or just Header Compression), which is an option in most versions of PPP. VJ is a data compression protocol described in RFC 1144, specifically designed by Van Jacobson to improve TCP/IP performance over slow serial links. The default value is disabled.

**See also**

create, delete, edit, glob, list, modify, net tunnels tunnel, regex, show, tmsh
tunnel

Configures a tunnel.

Module

net tunnels

Syntax

Configure the tunnel component within the net tunnels module using the following syntax.

Create/Modify

create tunnel [name]
modify tunnel [name]

options:
  auto-lasthop [default | enabled | disabled ]
  description [string]
  local-address [ip address]
  mode [bidirectional | inbound | outbound]
  mtu [integer]
  profile [ [name] | none]
  remote-address [ip address]
  tos [integer]

edit tunnel [ [ [name] | [glob] | [regex] ] ... ]

options:
  all-properties
  non-default-properties

Display

list tunnel
list tunnel [ [ [name] | [glob] | [regex] ] ... ]

show running-config tunnel
show running-config tunnel [ [ [name] | [glob] | [regex] ] ... ]

options:
  all-properties
  app-service
  non-default-properties
  one-line
  partition
Delete

delete tunnel [all | [name] ]

Description

You can use the `tunnel` component to configure a tunnel.

Examples

Creates a tunnel named `my_tunnel` between the local IP address `10.10.10.1` and the remote IP address `11.11.11.1`:

```
create tunnel my_tunnel local-address 10.10.10.1 remote-address 11.11.11.1 profile gre
```

Displays all of the properties of all of the tunnels:

```
list tunnel all-properties
```

Options

You can use these options with the `tunnel` component:

- **app-service**
  Displays the application service to which the object belongs. The default value is `none`.
  
  *Note: If the `strict-updates` option is enabled on the Application Service that owns the object, you cannot modify or delete the object. Only the Application Service can modify or delete the object.*

- **auto-lasthop**
  When enabled, specifies that the system returns packets to the MAC address from which they were sent. The default setting is `default`, which specifies that the system uses the default route to send back the request.

- **description**
  User-defined description.

- **glob**
  Displays the items that match the `glob` expression. For a description of `glob` expression syntax, see the `glob` man page.

- **local-address**
  Specifies a local IP address. This option is required.

- **mode**
  Specifies how the tunnel carries traffic. The default value is `bidirectional`.

- **mtu**
  Specifies the maximum transmission unit (MTU) of the tunnel. The default value is `0`. When the MTU is set to the default value (of `0`), the
MTU of the tunnel is computed by the system and is set to the MTU size of the underlying interface minus the encapsulation overhead introduced by the tunneling protocol. The valid range is 0 - 65535.

- **name**
  Specifies a unique name for the component. This option is required for the `create` and `modify` commands.

- **partition**
  Displays the administrative partition within which the component resides.

- **profile**
  Specifies the profile that you want to associate with the tunnel. This option is required for the `create` command.

- **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. For a description of regular expression syntax, see the `regex` man page.

- **remote-address**
  Specifies a remote IP address. This option is required for the `create` and `modify` commands.

- **tos**
  Specifies a value for insertion into the Type of Service (ToS) octet within the IP header of the encapsulating header of transmitted packets. The default value is `preserve`. The possible values are 0 (zero) - 255.

---

**See also**

create, delete, edit, glob, list, modify, net tunnels gre, net tunnels ipip, net tunnels wccp, regex, show, tmsh
**wccp**

Configures a Web Cache Communication Protocol (WCCP) GRE profile.

**Module**

*net tunnels*

**Syntax**

Configure the `wccp` component within the `net tunnels` module using the following syntax.

**Create/Modify**

```plaintext
create wccp [name]
modify wccp [name]

options:
  defaults-from [name]
  description [string]
  rx-csum [disabled | enabled]
  tx-csum [disabled | enabled]
  wccp-version [1 | 2]

edit wccp [ [ [name] | [glob] | [regex] ] ... ]

options:
  all-properties
  non-default-properties
```

**Display**

```plaintext
list wccp
list wccp [ [ [name] | [glob] | [regex] ] ... ]

show running-config wccp
show running-config wccp [ [ [name] | [glob] | [regex] ] ... ]

options:
  all-properties
  app-service
  non-default-properties
  one-line
  partition
```

**Delete**

```plaintext
delete wccp [all | [name] ]
```
Description

You can use the `wccp` component to create a WCCP GRE profile that you associate with a tunnel using the `tunnel` component. For more information about creating a tunnel, see `tunnel`, on page 38-14.

Examples

Creates a WCCP GRE profile named `my_wccp_gre`:

```plaintext
create wccp my_wccp_gre
```

Displays all of the properties of all of the WCCP GRE profiles:

```plaintext
list wccp all-properties
```

Options

You can use these options with the `wccp` component:

- **app-service**
  Displays the application service to which the object belongs. The default value is `none`.
  
  *Note:* If the `strict-updates` option is `enabled` on the Application Service that owns the object, you cannot modify or delete the object. Only the Application Service can modify or delete the object.

- **defaults-from**
  Specifies the existing profile from which the system imports settings for the new profile. The default value is `wccpgre`.

- **description**
  User-defined description.

- **glob**
  Displays the items that match the `glob` expression. For a description of `glob` expression syntax, see the `glob` man page.

- **name**
  Specifies a unique name for the component. This option is required for the `create` and `modify` commands.

- **partition**
  Displays the administrative partition within which the component resides.

- **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. For a description of regular expression syntax, see the `regex` man page.

- **rx-csum**
  Specifies whether the system verifies the checksum on received packets. The default value is `disabled`. 
◆ **rx-seqno**
  Specifies whether the system verifies the sequence number on received packets. The default value is disabled.

◆ **tx-csum**
  Specifies whether the system includes a checksum on transmitted packets. The default value is disabled.

◆ **tx-seqno**
  Specifies whether the system verifies the sequence number on transmitted packets. The default value is disabled.

◆ **wccp-version**
  Specifies the version of WCCP that the system uses. The default value is 2.

### See also

create, delete, edit, glob, list, modify, net tunnels gre, net tunnels ipip, net tunnels tunnel, regex, show, tmsh
sys Module Components

- Introducing the sys module
- Alphabetical list of components
Introducing the sys module

You can use the \texttt{tmsh} components that reside within the \texttt{sys} module to configure the BIG-IP® system settings and display information about the system. For more information about the \texttt{tmsh} hierarchical structure, see Chapter 2, \textit{Understanding and Using the Traffic Management Shell}.

Alphabetical list of components

The remainder of this chapter lists the \texttt{tmsh} components that are available in the \texttt{sys} module.
Chapter 39

**clock**

Displays the current date and time.

**Module**

**sys**

**Syntax**

Configure the *clock* component within the **sys** module using the following syntax.

**Display**

```
show clock
options:
  field-fmt
```

**Description**

You can use the *clock* component to display the system date and time.

**Examples**

Display the current date and time:

```
show clock
```

**Options**

For information about the options that you can use with the command *show*, see *show*, on page 3-39

**See also**

*show, tmsh*
cluster

Configures a cluster in a VIPRION® system.

Module

sys

Syntax

Configure the cluster component within the sys module using the following syntax.

Modify

modify cluster [name]
  options:
    address [IP address | none]
    [disabled | enabled]
    members {
      [1 | 2 | 3 | 4] {
        options:
          address [IP address | none]
          [disabled | enabled]
          priming [disabled | enabled]
        }
      }
    min-up-members [integer]
    min-up-members-enabled [no | yes]
edit cluster default
  options:
    all-properties
    non-default-properties

Display

list cluster
show running-config cluster
show running-config cluster [option name]
  options:
    one-line
show cluster
show cluster [option name]
  options:
    field-fmt
Description

You can use the **cluster** component to modify the configuration of the primary blade in a cluster. When you do this, the system automatically propagates the changes to the other blades in the cluster. This is known as cluster synchronization.

Examples

Sets the floating management IP address for cluster **default** to an IP address of **192.168.217.44**:

```
modify cluster default address 192.168.217.44/24
```

Disables the cluster named **my_cluster**:

```
modify cluster my_cluster disabled
```

Displays the properties of the cluster named **my_cluster**:

```
list cluster my_cluster
```

Options

You can use these options with the **cluster** component:

- **address**
  Specifies an IP address for the cluster or cluster member. The default value is **none**.

- **disabled**
  Disables the specified cluster or cluster member. The default value is **enabled**.

- **enabled**
  Enables the specified cluster or cluster member. This is the default value.

- **members**
  Specifies the cluster members to be acted on by the **cluster** component. A cluster member is a slot into which you insert a blade. The cluster member is identified by the number assigned to the slot.

- **min-up-members**
  Specifies the minimum number of cluster members that must be up for the cluster to remain active. The default value is **1**.

- **min-up-members-enabled**
  When set to **yes**, specifies when the number of cluster members that are active is below the value of the option **min-up-members**, the cluster fails over to its peer. The default value is **no**.

  Enable this parameter when you configure a redundant system configuration.
**Important:** Make sure that you modify the value of the `min-up-members` option appropriately when you take blades down in a cluster. Otherwise, you can get into the condition where disabling a cluster member brings the cluster below the value of the option `min-up-members`, which can cause the cluster to fail over to its peer.

- **name**
  Specifies a name for the cluster. This option is required for the `modify` command.

- **priming**
  Prevents a cluster member from proceeding to the RUNNING cluster quorum state, which is useful when a blade is in a reboot loop. The default value is `disabled`.

**See also**

`edit, list, modify, show, tmsh`
config

Manages the BIG-IP system configuration.

Module

sys

Syntax

Save the running configuration or load the system configuration files within the sys module using the following syntax.

Modify

save config
options:
    base
    binary
    file
    gtm-only
    one-line
    partitions
    tar-file
    time-stamp
    user-only
    wait
load config
options:
    base
    default
    file
    files-folder
    from-terminal
    gtm-only
    ltm-only
    merge
    partitions
    tar-file
    user-only
    verify
delete config file [file name]
Display

list config file

Description

The system applies all configuration changes that you make from within `tmsh` to the running configuration. To save the running configuration to the system configuration files, use the command sequence `save config`. Additionally, you can replace the running configuration with the configuration in the system configuration files using the command sequence `load config`.

Examples

Saves the running configuration in current update partition by overwriting the system configuration files:
```
save config
```

Saves the running base configuration in current update partition by overwriting the system base configuration files:
```
save config base
```

Saves all running configuration by overwriting the system binary configuration DB file:
```
save config binary
```

Save request waits if another save operation is in progress:
```
save config wait
```

Saves all running configuration to the specified file, `my_file`, and all the user provided disk files referred to by the configuration into `my_tar_file`:
```
save config file my_file tar-file my_tar_file
```

Saves the running configuration in `my_partition` by overwriting the system configuration files:
```
save config partitions { my_partition }
```

Saves the running configuration in all partitions by overwriting the system configuration files:
```
save config partitions all
```

Saves only user account configuration by overwriting the system configuration files:
```
save config user-only
```

Replaces the running configuration in current update partition with the configuration in the system configuration files:
```
load config
```
Chapter 39

Replaces the running base configuration in current update partition with the configuration in the system base configuration files:

```plaintext
load config base
```

Loads the specified configuration from `my_file`, which modifies the running configuration:

```plaintext
load config merge file my_file
```

Validates the specified configuration in `my_file` to see whether they are valid to replace the running configuration. The running configuration will not be changed:

```plaintext
load config verify file my_file
```

Validates the specified configurations in `my_file` to see whether they are valid to be merged into the running configuration. The running configuration will not be changed:

```plaintext
load config verify merge file my_file
```

Sets system configuration back to factory default settings:

```plaintext
load config default
```

Replace all running configuration with the configuration in the specified file, `my_file` and the disk files referred to by the configuration is retrieved from `my_tar_file`:

```plaintext
load config file my_file tar-file my_tar_file
```

Replace all running configurations with the configuration in the specified file, `my_file` and the disk files referred to by the configuration is taken from directory tree under `my_files_folder`.

While searching for `disk-file` under the specified folder, the order of search is first by file-name as in cache-path, and then by object-name. If more than one file is found for a name, then the relative path in the cache-path is used to make the selection.

That is, while looking for:

```plaintext
sys file ssl-cert xxx {
    cache-path
    /config/filestore/files_d/Common_d/certificate_d/xxx_1
    ...
}
```

Looks for file(s) by name `xxx_1`.

If none is found, looks for file(s) by name `x`

When more than one file is found, looks for a copy that matches paths in the order:

```plaintext
certificate_d/<name-found
Common_d/certificate_d/<name-found
load config file my_file files-folder my_files_folder
```
Replace the running configuration in partition \( x \) with the configuration in the system configuration files:

```bash
load config partitions { x }
```

Replace the running configuration in all partitions with the configuration in the system configuration files:

```bash
load config partitions all
```

Replace the running configuration with what is entered from the terminal.

1. Type the initial command:
   ```bash
   Load config from-terminal
   ```
   The system responds with a confirmation prompt, type Y to confirm.
   ```bash
   Replace the running configuration? (y/n) y
   ```

2. The system responds by prompting you to type in the replacement configuration entry:
   ```bash
   Enter configuration. Press CTRL-D to submit or CTRL-C to cancel.
   ```
   Type the replacement configuration entries.
   ```bash
   net self-allow {
   
   defaults {
     ospf: any
     tcp:161
     tcp:22
     tcp:4353
     tcp:443
     tcp:53
     udp:1026
     udp:161
     udp:4353
     udp:520
     udp:53
   }
   }
   
   net stp-globals {
     config-name 00-01-D7-B5-67-00
   }
   
   sys management-ip 172.27.41.70/24 {
   }
   
   sys management-route default {
     gateway 172.27.41.254
   }
   
   sys provision ltm {
     level nominal
   }
   ....
   ```
ltm pool pool1 {
    slow-ramp-time 200
}

^D:

3. Press Ctrl+D to submit the changes or Ctrl+C to cancel the changes.

Delete myfile in default directory, /var/local/scf/:

delete config file myfile

Display files in default directory, /var/local/scf/:

list config file

Options

You can use these options with the config command:

- **base**
  Indicates the base configuration. This option cannot be specified with binary, default, gtm-only, and user-only options.

- **binary**
  Indicates binary configuration. This option cannot be specified with any other options.

- **default**
  Indicates factory default configuration. This option cannot be specified with any other options.

- **file**
  Loads or saves a configuration from the specified file. For save, a file with a relative path is saved in the default directory, /var/local/scf. For load, in shell mode, the default directory, /var/local/scf, is used for a file with a relative path. In bash mode, for a file with a relative path, the current directory is searched first. If the file cannot be found in the current directory, /var/local/scf will be searched.

  This option can with binary, default, from-terminal and partitions.

- **tar-file**
  Loads or saves disk files referred to by the configuration from the specified tar file. A file with a relative path is looked up, relative to the current directory.

- **files-folder**
  Loads disk files referred to by the configuration from the folder tree under the specified folder. Disk files by name are searched for recursively. When there is more than one file with the same name, the relative path of the file from the cache-path is used for selection.
◆ **from-terminal**
Specifies that the configuration will be entered from the terminal in the same format as the system configuration files in /config. Use Ctrl+D to submit the changes and Ctrl+C to cancel the changes.
This option cannot be specified with the default, file, and partitions options.

◆ **gtm-only**
Indicates the Global Traffic Manager™ (GTM™) configuration. This option cannot be specified with the base, exclude-gtm, and user-only options.

◆ **exclude-gtm**
Indicates the BIG-IP configuration, excluding GTM devices. This is only valid with the file option. This option cannot be specified with the base, gtm-only, and user-only options.

◆ **merge**
Loads the configuration from the specified file or from the terminal, which modifies the running configuration. If merging from the terminal, it requires Ctrl+D to complete the operation. This option is only valid with the file or from-terminal options.

◆ **partitions**
Indicates the partitions in which configuration components reside. This option cannot be specified with the default, file, from-terminal, or merge options.

◆ **user-only**
Indicates the configuration, including user account information only. This option cannot be specified with the base, default, exclude-gtm, or gtm-only options.

◆ **time-stamp**
Inserts a time-stamp to a file name. This is only valid with the file option.

◆ **verify**
Validates the specified configuration from file(s) or from the terminal without changing the running configuration.

◆ **wait**
Indicates that tmsh should wait for another instance of tmsh to finish saving the configuration before proceeding. If wait is not specified and another instance of tmsh is in the process of saving the configuration, the command exits tmsh immediately (because the other instance of tmsh is already saving the configuration).

**See also**
load, save, tmsh
**config-diff**

Displays the differences between two specified single configuration files (SCFs).

**Module**

`sys`

**Syntax**

Display information using the `config-diff` component within the `sys` module with the syntax in the following section.

**Display**

```
show config-diff [file name] [file name]
```

**Description**

You can use the `config-diff` component to display the differences between two previously created SCF files.

**Examples**

Displays information about the differences between two files:

```
show config-diff my.scf your.scf
```

**Options**

You can use the following option with the `config-diff` component.

`file name`

Specifies the name of an SCF file that you want to compare to another SCF file.

**See also**

`save`, `tmsh`
connection

Sets idle timeout for, displays, and deletes active connections on the BIG-IP system.

Module

sys

Syntax

Use the connection component within the sys module to manage connections using the following syntax.

Modify

modify connection
  options:
    idle-timeout [integer]

Display

show connection
  options:
    all-properties
    age [integer]
    cs-client-addr [IP address]
    cs-client-port [ [integer] | [service] ]
    cs-server-addr [IP address]
    cs-server-port [ [integer] | [service] ]
    [default | exa | gig | kil | meg | peta | raw | tera | yotta | zetta]
    protocol [name]
    ss-server-addr [IP address]
    ss-server-port [ [integer] | [service] ]
    type [any | mirror | self]

Delete

delete connection
  option:
    age [integer]
    cs-client-addr [IP address]
    cs-client-port [ [integer] | [service] ]
    cs-server-addr [IP address]
    cs-server-port [ [integer] | [service] ]
```plaintext
protocol [name]
ss-server-addr [IP address]
ss-server-port [ [integer] | [service] ]
type [any | mirror | self]
```

### Description

You can use the `connection` component to set the idle timeout for or delete active connections to the BIG-IP system based on a specified filter. Additionally, you can display information about the active connections to the system.

You can specify the `port` option using either a number or a service (80 or http).

**Important**

*If you do not specify a port or service, the system deletes all connections that match just the IP address. If you do not specify an IP address, the system deletes all connections including mirrored connections.*

### Examples

Displays information about all active connections to the system:

```plaintext
show connection all-properties
```

Changes the amount of idle time before a connection is disconnected to five minutes (300 seconds):

```plaintext
modify connection idle-timeout 300
```

### Options

You can use the following options with the `connection` component:

- **age**
  Specifies, in seconds, the age of the active connections that you want to display or delete.

- **cs-client-addr**
  Specifies the clientside remote IP address of the active connections that you want to display or delete.

- **cs-client-port**
  Specifies the clientside remote port of the active connections that you want to display or delete.

- **cs-server-addr**
  Specifies the clientside local IP address of the active connections that you want to display or delete.
- **cs-server-port**
  Specifies the clientside local port of the active connections that you want to display or delete.

- **protocol**
  Specifies the protocol of the active connections that you want to display or delete.

- **ss-server-addr**
  Specifies the serverside remote IP address of the active connections that you want to display or delete.

- **ss-server-port**
  Specifies the serverside remote port of the active connections that you want to display or delete.

- **type**
  Specifies the type of active connections that you want to display or delete. The possible values are:
  - **any**
    Specifies all active connections.
  - **mirror**
    Specifies only mirrored connections.
  - **self**
    Specifies the connection with which you are accessing the system.

See also

`delete`, `modify`, `show`, `tmsh`
console

Configures the serial console on the BIG-IP system.

Module

sys

Syntax

Configure the console component within the sys module to manage connections using the following syntax.

Modify

modify console
  options:
    baud-rate [integer]

Display

show console

Description

You can use the console component to configure the serial console on the BIG-IP system.

Examples

Displays information about the serial console:

show console

Changes the baud rate on the serial console back to the default value of 19200:

modify console baud-rate 19200
Options

You can use the following option with the connection component:

**baud-rate**

Specifies the baud rate for the serial console. Select from the following options:

- **9600**
- **19200** (default)
- **57600**
- **11520**

For information about the options that you can use with the show command, see *show*, on page 3-39.

See also

- modify, show, tmsh
cpu

Displays statistics about the Traffic Management Microkernel (TMM) service, specifically CPU cycles.

Module

sys

Syntax

Display statistics for the cpu component within the sys module using the following syntax.

Display

show cpu

options:

  (default | exa | gig | kil | meg | peta | raw | tera | yotta | zetta)

  global

Description

You can use the cpu component to display the CPU cycles for the system. You can also specify the unit value in which the system displays statistics.

Examples

Displays TMM processor statistics in the system default units:

  show cpu

Displays raw TMM processor statistics:

  show cpu raw

Options

For information about the options that you can use with the show command, see show, on page 3-39.

See also

  show, tmsh
daemon-ha

Configures high availability for a BIG-IP system.

Module

sys

Syntax

Configure the daemon-ha component within the sys module using the following syntax.

Modify

modify daemon-ha [name]
options:
  heartbeat [enabled | disabled]
  heartbeat-action [go-offline | go-offline-downlinks-restart | go-offline-restart | \reboot | restart | restart-all]
  running [enabled | disabled]
edit daemon-ha [ [ [name] | [glob] | [regex] ] ... ]
options:
  all-properties
  non-default-properties

Display

list daemon-ha
list daemon-ha [ [ [name] | [glob] | [regex] ] ... ]
show running-config daemon-ha
show running-config daemon-ha [ [ [name] | [glob] | [regex] ] ... ]
options:
  all-properties
  non-default-properties
  not-running-action
  one-line
  running-timeout

Description

You can use the daemon-ha component to configure the daemons on the system that handle high availability for the BIG-IP system.
### Examples

Disables the `bigd` daemon:

```bash
modify daemon-ha bigd running disabled
```

Displays the running timeout of the `bigd` daemon:

```bash
list daemon-ha bigd running-timeout
```

### Options

You can use these options with the `daemon-ha` component:

- **glob**
  
  Displays the items that match the `glob` expression. For a description of `glob` expression syntax, see the `glob` man page.

- **heartbeat**
  
  Specifies whether heartbeat monitoring is enabled for the specified daemon. If monitoring is enabled and the daemon does not maintain its heartbeat the action specified by the value of the `heartbeat-action` option is taken.

  The default value is **enabled** for all daemons, except the `named` daemon, which is **disabled** by default.

- **heartbeat-action**
  
  Specifies the action the system takes if the specified daemon does not maintain its heartbeat.

  The default value is dependent on the specified daemon, the most common default value is **restart**.

- **name**
  
  Specifies a unique name for the component. This option is required for the commands `modify`.

- **not-running-action**
  
  Specifies the action that the system takes if the daemon is not running. This option is read-only.

  The default value is dependent on the specified daemon, the most common default value is **go-offline-downlinks**.

- **regex**
  
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. For a description of regular expression syntax, see the `regex` man page.

- **running**
  
  Specifies whether the `running-timeout` and `non-running-action` options are **enabled**. The default value is dependent on the specified daemon, the most common default value is **enabled**.

  **Note:** This feature is implemented only for the daemons: `tmn`, `mcpd`, `bcm56xxd`, `gtmd`, `clusterd`, `named`, and `tmrouted`. 
◆ running-timeout
   Specifies the amount of time (in seconds) that must elapse before the
   specified daemon is considered to be not running. This option is
   read-only. The default value is dependent on the specified daemon.

See also

e, gl, ls, md, re, s, tmsh
**datastor**

Configures the data storage used for optimization.

**Module**

sys

**Syntax**

Configure the `datastor` component within the sys module using the following syntax.

**Modify**

```bash
modify datastor
options:
  description [string]
  disk [disabled | enabled]
  high-water-mark [integer]
  low-water-mark [integer]
```

**Display**

```bash
list datastor
show running-config datastor
options:
  all-properties
  cache-size
  non-default properties
  one-line
  store-size
```

**Description**

You can use the `datastor` component to configure disk I/O operations and optimized page cache for frequently accessed sectors. Note that symmetric data deduplication is one consumer of this storage space.

**Examples**

Displays the data storage settings:

```bash
list datastor all-properties
```
Disables data storage on the disk:

```
modify datastor disk disabled
```

**Options**

You can use these options with the `datastor` component:

- **cache-size**
  Displays the size of the data storage in megabytes (MB).

- **description**
  User-defined description.

- **disk**
  Enables or disables the use of the disk (in addition to memory) for data storage.
  
  If you enable or disable data storage on the disk, you must then restart the `datastor` service from the command line using the command sequence `bigstart restart datastor`.

- **high-water-mark**
  Specifies the percentage of full cache above which pruning starts. The valid range is from 60 to 100 percent. The default value is 92.

- **low-water mark**
  Specifies the percentage of full cache below which pruning stops. The valid range is from 10 to 90 percent. The default value is 80.

- **store-size**
  Displays the amount of space for each disk path specified.

**See also**

- `list`, `modify`, `show`, `tmsh`, `wom deduplication`
db

Displays or modifies bigdb database entries.

Module

sys

Syntax

Configure the db component within the sys module using the following syntax.

Modify

modify db [name] value [database variable value]

Display

list db
list db [ [ [name] | [glob] | [regex] ] ... ]
options:
  all-properties
  default-value
  non-default-properties
  one-line
  value
  value-range

show running-config db
show running-config db[ [ [name] | [glob] | [regex] ] ... ]
options:
  all-properties
Description

You can use the `db` component to modify and retrieve the data that is stored in the bigdb configuration database.

**Important**

After you change a bigdb database variable using the `db` component, you must type the command sequence `save config`. If you do not, the next time that you type the command sequence `load [base-config | config]`, the value of the bigdb database variable might be reset to the value in the stored configuration.

**Note**

`tmsh` displays bigdb database entries only when you explicitly request them.

Examples

Sets the database entry, SYN Check™ Activation Threshold, back to the default value:

```
modify db Connection.SynCookies.Threshold value 16384
```

Displays the properties of the database entry `log.mcpd.level`:

```
list log.mcpd.level
```

Options

You can use these options with the `db` component:

- **default-value**
  Displays the system-supplied default value of the database entry.

- **glob**
  Displays the items that match the `glob` expression. For a description of `glob` expression syntax, see the `glob` man page.

- **name**
  Specifies the unique name of the database entry. This option is required for the `modify` command.

- **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (`@`[regular expression]) to indicate that the identifier is a regular expression. For a description of regular expression syntax, see the `regex` man page.
◆ value
   Specifies the value to which you want to set the specified database entry.

◆ value-range
   Displays the type of data that you can use with the value option.
   The options are:
   • integer
   • IP address
   • list of valid values
   • management IP address
   • string
   • unsigned integer

See also

glob, list, modify, regex, show, tmsh
**default-config**

Loads the default configuration of the BIG-IP system stored in the configuration files to the running configuration of the system.

**Module**

sys

**Syntax**

Configure the default-config component within the sys module using the following syntax.

**Modify**

load default-config

**Description**

You can use the default-config component to load the default system configuration to the running configuration. This results in the user-defined configuration being removed from the running configuration.

**Examples**

Loads the default configuration stored on the system to the running configuration of the system:

load default-config

**See also**

load, tmsh
The `dns` component in the `sys` module is used to configure the Domain Name System (DNS) for the BIG-IP system.

### Syntax

Configure the `dns` component within the `sys` module using the following syntax:

#### Modify

```
modify dns
  options:
    description [string]
    include [string]
    name-servers [add | delete | replace-all-with] { [ip address] ... }
    name-servers none
    search [add | delete | replace-all-with] { [domain] ... }
    search none
```

#### Edit

```
edit dns
  options:
    all-properties
    non-default-properties
```

### Display

```
list dns
list dns [option]
show running-config dns
show running-config dns [option]
  options:
    all-properties
    non-default-properties
    one-line
```

### Description

You can use the `dns` component to manage configurations by server grouping, in this case, DNS servers.
Examples

Adds DNS name servers with the IP addresses 192.168.10.20 and 192.168.10.22 to the BIG-IP system:

```bash
modify dns name-servers add { 192.168.10.20 192.168.10.22 }
```

Adds the host names siterequest.com, store.siterequest.com, and london.siterequest.com to the DNS search configuration for the BIG-IP system.

```bash
modify dns search add { siterequest.com store.siterequest.com london.siterequest.com }
```

◆ Note

When DNS searches for the host, siterequest, which is not a fully qualified domain name, it uses the IP address of the first match (in this case, siterequest.com).

Displays the running configuration of the dns component:

```bash
show running-configuration dns
```

Options

You can use these options with the dns component:

◆ description
  User-defined description.

◆ include

  Warning: Do not use this option without assistance from the F5 Technical Support team. The system does not validate the commands issued using the include option. If you use this option incorrectly, you put the functionality of the system at risk.

◆ name-servers
  Configures a group of DNS name servers for the BIG-IP system.

◆ search
  Configures a list of domain names in a specific order. DNS uses that order when searching for host names that are not fully qualified. You can use this option to delete domain names in the list.

See also

edit, list, modify, show, tmsh
failover

Configures failover for a BIG-IP unit in a redundant system configuration.

Module

sys

Syntax

Configure the failover component within the sys module using the syntax in the following section.

Modify

run failover
  options:
    device [string]
    no-persist
    offline
    online
    persist
    standby
    traffic-group [string]

Display

show failover
  options:
    cable

Description

Failover is the process where a standby unit in a redundant system configuration takes over when a software or hardware failure is detected on the active unit.

Examples

Causes the active unit or cluster into the standby state, forcing the other unit or cluster in the redundant system configuration to become active:

run failover standby
Causes the active unit or cluster to change into the Forced Offline state:

```
run failover offline
```

Changes the status of a unit or cluster from Forced Offline to either Active or Standby, depending upon the status of the other unit or cluster in a redundant system configuration

```
run failover online
```

Displays the failover state of the BIG-IP system (active, standby, offline) and how long it has been in that state:

```
show failover
```

The `my_bigip` device becomes the active device for all traffic groups:

```
run failover standby device my_bigip
```

The traffic group named `traffic_grp01` fails over to the Standby state. The traffic group will then become Active on another device:

```
run failover standby traffic-group traffic_grp01
```

Changes the status of a unit to Forced Offline and indicates that the change will not be persisted after a system restart:

```
run sys failover offline no-persist
```

Changes the status of a unit to Forced Offline and indicates that the change will be persisted after a system restart

```
run sys failover offline persist
```

**Options**

Use these options to control failover of the system:

- **device**
  Specifies the device that should next become the active device for the specified traffic group or all traffic groups (if a traffic group is not specified). This option can only be specified with the `standby` option.

- **no-persist**
  Does not persist the change in status of a unit. The option is valid only with the `offline` state.

- **offline**
  Changes the status of a unit or cluster to Forced Offline. If the `persist` or `no-persist` options are not specified, the default action is to persist the offline status of the unit between system restarts.

- **online**
  Changes the status of a unit or cluster from Forced Offline to either Active or Standby, depending upon the status of the other unit or cluster in a redundant system configuration.

- **persist**
  Persists the change in status of a unit. The option is valid only with the `offline` state.
◆ **standby**
  Indicates that the active unit or cluster fails over to a Standby state, causing the standby unit or cluster to become Active.

◆ **traffic-group**
  Indicates that the traffic-group that should fail over to the Standby state, the traffic-group will become Active on another device. This option can only be specified with the standby option.

Use this option to display failover cable status of the system:

◆ **cable**
  Displays the status that the failover daemon detects on the serial cable from its failover peer. It also shows what the failover peer detects on the serial cable. An active BIG-IP system will see a 0 from its failover peer. A standby BIG-IP system will see a 1 from its failover peer.

**See also**

run, tmsh
folder

Configure folders (directory structure) on the BIG-IP system.

Module

sys

Syntax

Configure the folder component within the sys module using the following syntax.

Create/Modify

create folder [name]
modify folder [name]
  options:
    description [string]
    device-group [name | none]
    no-ref-check [false | true]
    traffic-group [name | none]

Display

list folder
list folder [ [name] | [glob] | [regex] | [recursive] ]

Delete

delete folder [name]

Description

The folder system enables users to create logical containers for the purpose of granular control of synchronization to other devices in a device group.

The folder system is hierarchical, with folders and sub-folders, in a parent-to-child relationship. The highest level folder in the system is called root. For every administrative partition on the BIG-IP system, there is a top-level folder. Top-level folders always have root as the parent. Users can create sub-folders to any folder in the system.
Examples

Creates a new sub-folder to the current working folder called sub-folder1, associates the folder with a device-group called dg1, and sets the traffic-group to no association:

```
create sys folder sub-folder1 device-group dg1 traffic-group none
```

Changes the description property of the folder indicated by its full name:

```
modify sys folder /Common/sub-folder1/subfolder2 description "store pools for the B2 server configuration"
```

Options

You can use the following options with the folder component:

- **description**
  User-defined description.

- **device-group**
  Adds this folder and all configuration items in this folder to a device-group for network failover or config-sync purposes. The options are:
  - **default**
    Indicates that this folder should use the device group setting of its parent folder. If the parent folder's associated device group is changed, this folder's device group will change as well.
  - **non-default**
    Dissociates this folder from its parent folder's device group setting. This folder's device group field can then be set independently of the parent folder's field.

- **inherited-devicegroup**
  Specifies, when set to true, that this folder uses the device group setting of its parent folder. If the parent folder's associated device group is changed, then this folder's device group will change as well. This field is read-only.

- **inherited-traffic-group**
  Specifies, when set to true, that this folder uses the traffic group setting of its parent folder. If the parent folder's associated traffic group is changed, then this folder's traffic group will change as well. This field is read-only.

- **no-ref-check**
  Specifies whether strict device group reference validation is performed on configuration items in the folder.
    - **false**
      Requires configuration items in the folder to sync to a super-set of the devices that are associated with any configuration that refers to configuration items in the folder. This is the default value.
• **true**
  Disables this check. Then, any dependent configuration items contained in the folder will be created locally on the other devices.

• **traffic-group**
  Adds this folder and its configuration items to a device failover group. The values **default** and **non-default** work as they do for the **device-group** option.

**See also**

create, delete, device-group, glob, list, modify, regex, traffic-group, tmsh
geoip

Loads the GeoIP data files.

Module

sys

Syntax

Use the geoip component within the sys module to load the GeoIP data files using the syntax in the following sections.

Modify

Loads the GeoIP files from disk into the running configuration:

```
load geoip
```

Description

The BIG-IP system ships with three default database files that are stored in the /usr/share/GeoIP/ directory. The three files are: F5GeoIP.dat, F5GeoIPISP.dat, and F5GeoIPv6.dat.

You can download and install updated GeoIP database files using the procedure available from the F5 download site. The installation places the updated database files in the share/GeoIP directory.

When you run the load geoip command sequence, the system loads the GeoIP files from disk into the running configuration. If you have downloaded and installed updated database files, those files are loaded from the /shared/GeoIP directory. Otherwise, the default database files are loaded from the /usr/share/GeoIP/ directory. Note that if both directories contain the same files, the files in shared/GeoIP are loaded.

Examples

Loads the GeoIP files from disk into the running configuration:

```
load geoip
```

See also

load, tmsh
global-settings

Configures the global system settings for a BIG-IP system.

Module

sys

Syntax

Configure the global-settings component within the sys module using the following syntax.

Modify

modify global-settings

options:
  archive-encrypt [on | on-request | off]
  auth-source-type [local | ldap | radius | active-directory | tacacs]
  clustered [disabled | enabled]
  clustered-primary [disabled | enabled]
  console-inactivity-timeout [integer]
  custom-addr [IP address]
  failsafe-action [go-offline | reboot | restart-all |
    go-offline-restart-tm | failover-restart-tm]
  gui-security-banner [disabled | enabled]
  gui-security-banner-text [string]
  gui-setup [disabled | enabled]
  host-addr-mode [custom | management | state-mirror]
  hostname [string]
  hosts-allow-include [string]
  lcd-display [disabled | enabled]
  net-reboot [disabled | enabled]
  password-prompt [string]
  quiet-boot [disabled | enabled]
  remote-host [add | delete | replace-all-with] {
    [name]... {
      options:
      addr [IP address]
      hostname [string]
    }
  }
  remote-host none
  username-prompt [string]
**edit global-settings**

**options:**
- all-properties
- non-default-properties

**Display**

```plaintext
list global-settings
list global-settings [option name]
show running-config global-settings
show running-config global-settings [option name]
options:
- all-properties
- non-default-properties
- one-line
```

**Description**

You can use the `global-settings` component to set up the BIG-IP system.

**Examples**

Sets up a remote host named `bigip151` with an IP address of `172.27.226.151` and a hostname of `bigip151.saxon.net`:

```plaintext
modify system remote-host add {
  bigip151 {addr 172.27.226.151 hostname bigip151.saxon.net}
}
```

Displays all of the properties of the global system settings:

```plaintext
list global-settings all-properties
```

**Options**

You can use these options with the `global-settings` component:

- **archive-encrypt**
  
  Specifies the state of the system archive encryption feature. The default value is `on-request`.

  You must configure this option in conjunction with the `encrypt` and `passphrase` options of the `sys config-sync` component. The reason for this is when you perform a configuration synchronization of two units in a redundant system configuration, the process involves saving a `*.ucs` file from one system onto the peer system, and then installing the saved file on the peer system. You use the `archive-encrypt` option of the `sys global-settings` component to indicate whether the process of saving the `*.ucs` file creates an encrypted or unencrypted file.
For example, you can set the encrypt option of the sys config-sync component to enabled and configure a value for the passphrase option of the sys config-sync component. If you use the default value, on-request, for the archive-encrypt option of the sys global-settings option, then when a user saves the *.ucs file and provides the passphrase, the *.ucs file is encrypted. If the user does not provide the passphrase, the *.ucs file is not encrypted.

- **auth-source-type**
  Specifies the default user authorization source. The default value is local. When user accounts that access the system reside on a remote server, the value of the this option is the type of server that you are using for authentication, for example: ldap.

- **clustered**
  Enables or disables clustering on a VPRION system.

- **clustered-primary**
  Specifies whether the specified cluster is the primary cluster.

- **console-inactivity-timeout**
  Specifies the number of seconds of inactivity before the system logs off a user that is logged on. The default value is 0 (zero), which means that no timeout is set. The valid range is 0 - 2147483647.

- **custom-addr**
  Specifies an IP address for the system. The default value is ::. Note: If you specify an IP address using this option, you must also set the host-addr-mode option to custom.

- **failsafe-action**
  Specifies the action that the system takes when the switch board fails. The default value is go-offline-restart-tm. The possible values are:
  - **failover-restart-tm**
    When the switch board fails, the system restarts the traffic management system and fails over to the other unit in a redundant pair.
  - **go-offline**
    When the switch board fails, the system goes offline.
  - **go-offline-restart-tm**
    When the switch board fails, the system goes offline and restarts the traffic management system.
  - **reboot**
    After the active cluster fails over to its peer, it reboots while the peer processes the traffic.
  - **restart-all**
    When the switch board fails, the system restarts all system services.

- **gui-security-banner**
  Specifies whether the system presents on the login screen the text you specify in the gui-security-banner-text option. If you disable this option, the system presents an empty frame in the right portion of the login screen. The default value is enabled.
◆ gui-security-banner-text
Specifies the text to present on the login screen when the gui-security-banner option is enabled. The default value is Welcome to the BIG-IP Configuration Utility.

*Note:* To enter a carriage return in the text, type Ctrl + V followed by Ctrl + J. Additionally, you must escape special characters, such as a question mark (?), with a back slash.

◆ gui-setup
Enables or disables the Setup utility in the browser-based Configuration utility. The default value is enabled.

*Note:* When you configure a system using the `tmsh` utility, disable this option. Disabling this option allows the system administrators to use the browser-based Configuration utility without having to run the Setup utility.

◆ host-addr-mode
Specifies the type of host address you want to assign to the system. The default value is management. The possible values are:

- custom
  Use this value when you want to specify a custom IP address for the system using the custom-addr option.

- management
  Indicates that the host address is the management port of the system.

- state-mirror
  Use this value when the host address of the system is shared by the other system in a redundant system configuration. In case of system failure, the traffic to the other system is routed to this system.

◆ hostname
Specifies a local name for the system. The default value is bigip1.

◆ hosts-allow-include
*Warning:* Do not use this parameter without assistance from the F5 Technical Support team. The system does not validate the commands issued when you use the hosts-allow-include option. If you use this option incorrectly, you put the functionality of the system at risk.

◆ lcd-display
Enables or disables the LCD display on the front of the system. The default value is enabled.

◆ net-reboot
Enables or disables the network reboot feature. The default value is disabled.

If you enable this feature and then reboot the system, the system boots from an ISO image on the network, rather than from an internal media drive. Use this option only when you want to install software on the system, for example: for an upgrade or a re-installation.

*Note:* An enabled value reverts to disabled after you reboot the system a second time.
◆ **password-prompt**
Specifies the text to present above the password field on the system's login screen.

◆ **mgmt-dhcp**
Specifies whether the system uses DHCP client for acquiring the management interface IP address. If this option is enabled, manually specified IP addresses for the management interface can be overwritten if the network also contains a DHCP server. If this option is disabled, no DHCP server will be applied to the management interface, however any previously acquired address will still be used. The default value is disabled.

◆ **quiet-boot**
Enables or disables the quiet boot feature. The default value is **enabled**. When **enabled**, the system suppresses informational text on the console during the boot cycle.

◆ **remote-host**
Configures a remote host in the `/etc/hosts` file. The default value is **none**. You must enter both an IP address and a fully qualified domain name (FQDN) or alias for each host that you want to add to the file.

◆ **username-prompt**
Specifies the text to present above the user name field on the system's login screen.

### See also

`edit`, `list`, `modify`, `show`, `tmsh`
**ha-group**

Configures the high availability (HA) scoring mechanism for a unit in a redundant system configuration.

**Module**

sys

**Syntax**

Configure the ha-group component within the sys module using the following syntax.

**Create/Modify**

```plaintext
create ha-group [name]
modify ha-group [name]
  options:
  - active-bonus [integer]
  - clusters none
  - clusters [add | delete | modify | replace-all-with] {
    [name] {
      attribute percent-up-members
      threshold [integer]
      weight [integer]
    }
  }
  description [string]
  [disabled | enabled]
  pools none
  pools [add | delete | modify | replace-all-with] {
    [name] {
      attribute percent-up-members
      threshold [integer]
      weight [integer]
    }
  }
  trunks none
  trunks [add | delete | modify | replace-all-with] {
    [name] {
      attribute percent-up-members
      threshold [integer]
      weight [integer]
    }
  }
```
Display

list ha-group
list ha-group [name]

options:
   one-line

Delete

delete ha-group [name]

Description

You can use the ha-group component to configure a high availability (HA) group that determines the scoring mechanism for a unit in a redundant system configuration. This mechanism compares the relative health of the two units and the system with the highest score becomes the active unit.

Examples

Creates a HA group, named group1, that includes the pool named ftp_pool and uses the attribute percent-up-members and a weight of 70 to determine the HA score for a unit in a redundant system configuration:

create ha-group group1 pools add { ftp_pool { attribute percent-up-members weight 70 } }

Displays the configuration of the HA group, group1:

list ha-group group1

Options

You can use the following options with the ha-group component:

◆ active-bonus
   Specifies a number to add to the unit’s HA score when the unit is active. This option ensures that the state of a unit is dependent upon the history of its state. The default value is 10 (ten). The range is 0 - 100.

◆ attribute
   Specifies an attribute of the component that you want to use for the HA scoring mechanism. Percent-up-members is the only available attribute for HA scoring for the clusters, pools, and trunks options.

◆ clusters
   Specifies the clusters that you want to configure for the HA group. You can only configure a cluster on a chassis.

◆ description
   User-defined description.
◆ [disabled | enabled]
Enables or disables the HA group in the HA table. The default value is enabled.

◆ name
Specifies the name of the component that you want to configure. This option is required when you create, modify, or delete a HA group. This option is also required when you configure clusters, pools, or trunks for the HA group.

◆ pools
Specifies the pools that you want to configure for the HA group.

◆ threshold
Specifies the minimum number of up interfaces in the trunk, up pool members in the pool, or up cluster members in the cluster below, which the specified component does not contribute to the HA score for the unit. The default value is 0 (zero), which indicates this option is disabled. The value cannot exceed the number of members of the trunk, pool, or cluster.

◆ trunks
Specifies the interfaces that you want to configure for the HA group.

◆ weight
The value of this option is multiplied by the percent of up cluster, pool, or trunk members, and is added to the HA score. The default value is 10. The range is 10 - 100.

See also

create, delete, list, modify, tmsh
**hardware**

Displays information about the BIG-IP system hardware.

**Module**

*sys*

**Syntax**

Display statistics for the **hardware** component within the **sys** module using the following syntax.

```plaintext
show hardware
```

**Description**

You can use the **hardware** component to display information about the hardware.

**Examples**

Displays hardware information for the system:

```plaintext
show hardware
```

**Options**

For information about the options that you can use with the **show** command, see **show**, on page 3-39.

**See also**

*show, tmsh*
**ha-status**

Displays information about the high availability (HA) status of a unit in a redundant system configuration.

**Module**

sys

**Syntax**

Use the ha-status component within the sys module to display high-availability status using the following syntax.

**Display**

```plaintext
show ha-status
```

**Options:**

```plaintext
options:
  all-properties
  (default | exa | gig | kil | meg | peta | raw | tera | yotta | zetta)
  field-fmt
```

**Description**

You can use the ha-status component to display information about the high availability (HA) status of a unit in a redundant system configuration.

**Examples**

Displays information about the HA status of the unit:

```plaintext
show ha-status
```

**Options**

For information about the options that you can use with the show command, see show, on page 3-39.

**See also**

show, tmsh
**host-info**

Displays statistics about the host.

**Module**

sys

**Syntax**

Display statistics for the **host-info** component within the sys module using the following syntax.

```
show host-info
```

**Description**

You can use the **host-info** component to display statistics about the host, including CPU count, active CPU count, processor mode, memory usage, and more.

**Examples**

Displays host statistics in the system default units:

```
show host-info
```

Displays raw host statistics:

```
show host-info raw
```

**Options**

For information about the options that you can use with the **show** command, see **show**, on page 3-39.

**See also**

**show, tmsh**
httpd

Configures the HTTP daemon for the BIG-IP system.

Module

sys

Syntax

Configure the httpd component within the sys module using the following syntax.

Create/Modify

modify httpd [name]

options:
  allow [add | delete | none | replace-all-with] { hostname or IP address ... }
  auth-name [string]
  auth-pam-dashboard-timeout [disabled | enabled]
  auth-pam-idle-timeout [integer]
  description [string]
  fastcgi-timeout [integer]
  hostname-lookup [double | off | on]
  include [string]
  log-level [alert | crit | debug | emerg | error | info | notice | warn]
  redirect-http-to-https [disabled | enabled]
  ssl-ca-cert-file [string]
  ssl-certificatefile [string]
  ssl-certkeyfile [string]
  ssl-ciphersuite [string]
  ssl-include [string]
  ssl-verify-client [no | require | optional | optional-no-ca]
  ssl-verify-depth [integer]
  ssl-ocsp-enable [on | off]
  ssl-ocsp-default-responder [string]
  ssl-ocsp-override-responder [on | off]

edit httpd

options:
  all-properties
  non-default-properties
Display

```
list httpd
list httpd [option name]
show running-config httpd
show running-config httpd [name]
```

**options:**
- all-properties
- non-default-properties
- one-line

Description

You can use the `httpd` component to configure the HTTP daemon for the system.

**Important**

_F5 Networks recommends that users of the Configuration utility exit the utility before changes are made to the system using the `httpd` component. This is because making changes to the system using this component causes a restart of the `httpd` daemon. Additionally, restarting the `httpd` daemon requires a restart of the Configuration utility._

Examples

Changes the SSL certificate and the SSL key. When you change the SSL key, you must also change the SSL certificate:

```
modify httpd { ssl-certfile [string] ssl-certkeyfile [string] }
```

Sets the PAM idle timeout to half a day (in seconds):

```
modify httpd auth-pam-idle-timeout 43200
```

Replaces the existing list of hosts that can connect to the `httpd` daemon with the hosts in the range, _172.27.0.0/255.255.0.0_:

```
modify httpd auth-pam-idle-timeout 43200
```

Options

You can use these options with the `httpd` component:

- **allow**
  - Configures IP addresses and hostnames for the HTTP clients from which the `httpd` daemon accepts requests. The default value is _All_.
  - **Warning:** Using the value _none_ resets the `httpd` daemon to allow all HTTP clients access to the system; therefore, _F5 Networks recommends that you do not use the value none_.

---

◆ **auth-name**
   Specifies the name for the authentication realm. The default value is **BIG-IP**.

◆ **auth-pam-dashboard-timeout**
   Specifies whether browser session timeout occurs when the dashboard is running. The default value is **disabled**.

◆ **auth-pam-idle-timeout**
   Specifies the number of seconds of inactivity that can elapse before the GUI session is automatically logged out. The default value is **1200** seconds.

◆ **description**
   User-defined description.

◆ **fastcgi-timeout**
   Specifies, in seconds, the timeout for FastCGI. The default value is **300** seconds.

◆ **hostname-lookup**
   Specifies whether the hostname lookup feature is off or on. The default value is **off**.

◆ **include**
   The default value is **none**.

   **Warning:** Do not use this option without assistance from the F5 Technical Support team. The system does not validate the commands issued using this option. If you use the include option incorrectly, you put the functionality of the system at risk.

◆ **log-level**
   Specifies the minimum **httpd** message level to include in the system log. The default value is **warn**.

◆ **redirect-http-to-https**
   Specifies whether the system should redirect HTTP requests targeted at the configuration utility to HTTPS. The default value is **disabled**.

◆ **ssl-ca-cert-file**
   Specifies the name of the file that contains the SSL Certificate Authority (CA) certificate file. The default value is **none**.

◆ **ssl-certchainfile**
   Specifies the name of the file that contains the SSL certificate chain. The default value is **none**.

◆ **ssl-certfile**
   Specifies the name of the file that contains the SSL certificate. The default value is `/etc/httpd/conf/ssl.crt/server.crt`.

   Note that the path to the file must start with either `/etc/httpd/conf/ssl.crt/` or `/config/httpd/conf/ssl.crt/`, unless the path is a relative path. If the path is a relative path, then it must start with `config/ssl.crt/`.

◆ **ssl-certkeyfile**
   Specifies the name of the file that contains the SSL certificate key. The default value is `/etc/httpd/conf/ssl.key/server.key`. 
Note that the path to the file must start with either /etc/httpd/conf/ssl.key/ or /config/httpd/conf/ssl.key/, unless the path is a relative path. If the path is a relative path, then it must start with conf/ssl.key/.

When you change the key file, you must also change the certificate file. For example, use the following command sequence to change the key: modify httpd { ssl-certfile [string] ssl-certkeyfile [string] }

- **ssl-ciphersuite**
  Specifies the ciphers that the system uses. The default value is “ALL:!ADH:!EXPORT56:!eNULL:!MD5:RC4+RSA:+HIGH:+MEDIUM:+LOW:+SSLv2:+EXP”

- **ssl-include**
  The default value is none.

  **Warning:** Do not use this option without assistance from the F5 Technical Support team. The system does not validate the commands issued using this option. If you use the ssl-include option incorrectly, you put the functionality of the system at risk.

- **ssl-ocsp-default-responder**
  Specifies the default responder URI for OCSP validation. The default is http://localhost.localdomain. The value for the default responder should always be preceded with http://.

- **ssl-ocsp-enable**
  Specifies OCSP validation of the client certificate chain. The default is off.

- **ssl-ocsp-override-responder**
  Specifies the force use of default responder URI for OCSP validation. The default is off.

- **ssl-verify-client**
  Specifies if the client certificate needs to be verified for SSL session establishment. The default is no.

- **ssl-verify-depth**
  Specifies maximum depth of CA certificates in client certificate verification. The default is 10.

**See also**

edit, list, modify, show, tmsh
hypervisor-info

Displays configuration information passed to a guest from the hypervisor.

Module

sys

Syntax

Access the hypervisor-info component within the sys module using the syntax in the following sections.

Display

show hypervisor-info

options:

(default | exa | gig | kil | meg | peta | raw | tera | yotta | zetta)

field-fmt

Description

You can use the hypervisor-info component to display guest configuration information suggested by the hypervisor.

Examples

Displays hypervisor configuration information in default units:

show hypervisor-info

Options

For information about the options that you can use with the show command, see show, on page 3-39.

See also

show, tmsh
**icmp-stat**

Displays and resets ICMP statistics on the BIG-IP system.

**Module**

sys

**Syntax**

Display statistics for the **icmp-stat** component within the **sys** module using the syntax in the following section.

**Modify**

reset-stats icmp-stat

**Display**

```
show cpu
  options:
    (default | exa | gig | kil | meg | peta | raw | tera | yotta | zetta)
  global
```

**Description**

You can use the **icmp-stat** component to display and reset ICMP statistics. The statistics you can view are standard ICMP statistics, including ICMPv4 packets and errors, and ICMPv6 packets and errors.

**Options**

For information about the options that you can use with the **show** command, see **show**, on page 3-39.

**See also**

reset-stats, show, sys icmp-stat, tmsh
ip-address

Displays all IP addresses currently associated with a configuration object on a BIG-IP system.

Module

sys

Syntax

Display the IP addresses associated with a BIG-IP system configuration object using the syntax in the following section.

Display

show ip-address
options:
   [all-properties | field-fmt]

Description

You can use the ip-address component to display the location on the BIG-IP system of the IP addresses associated with a configuration object. The system displays the following information:

◆ Entry
   Displays the IP address and any associated configuration. For example, for a Local Traffic Manager™ pool member, the entry is the member's IP address and port number, 10.1.1.1:80.

◆ Component
   Displays the type of component associated with the IP address. For example, for a Local Traffic Manager pool, the entry is ltm pool.

◆ Object-ID
   Displays the name of a configuration object associated with the IP address. For example, for a Local Traffic Manager pool named my_pool, the entry is my_pool.

◆ Property
   When you specify the all-properties option, displays the name of the property that contains the IP address value. If the IP address is an object identifier the system displays n/a.
Examples

Displays the IP addresses currently associated with a BIG-IP system configuration object:

```
show ip-address
```

Options

For information about the options that you can use with the `show` command, see `show`, on page 3-39.

See also

```
show, tmsh
```
iprep-status

Displays the status of an IP reputation database. In the BIG-IP Configuration utility, this database is referred to as the IP Address Intelligence database.

Module

sys

Syntax

Configure the iprep-status component within the sys module using the syntax shown in the following sections.

Display

show iprep-status
options:
  field-fmt

Description

You can use the iprep-status component to display status information about the IP reputation database. The reputation database (referred to as IP Address Intelligence in the Config utility) is available from third-party vendors. An IP intelligence database is a list of IP addresses that have a questionable reputation. The status information returned includes:

- the date and time that the BIG-IP system last contacted the vendor server
- the date and time that the BIG-IP system last received an update
- the total number of IP address in the database
- the number of IP addresses in the most recent update

When the system has an IP Intelligence license and the database variable db iprep.autoupdate is enabled (default), the database is automatically downloaded and stored in the binary file:

/var/IpRep/F5IpRep.dat

The database contains information that maps IP addresses or ranges of IP addresses to one or more reputation categories. After every update, the IpRep data file is loaded from disk into the running configuration.
Examples

Displays current status information for the IP reputation database

show iprep-status

Options

For information about the options that you can use with the command show, see help show.

See also

show, tmsh
ip-stat

Displays and resets IP statistics on the BIG-IP system.

Module

sys

Syntax

Configure the ip-stat component within the sys module using the syntax in the following section.

Modify

reset-stats ip-stat

Display

show ip-stat
  options:
    (default | exa | gig | kil | meg | peta | raw | terra | yotta | zetta)

Description

You can use the ip-stat component to display and reset IP statistics. The statistics you can view are standard IP statistics, including IPv4 and IPv6 packets, fragments, fragments reassembled, and errors.

Options

For information about the options that you can use with the show command, see show, on page 3-39.

For information about the options that you can use with the command reset-stats, see reset-stats, on page 3-31.

See also

reset-stats, show, sys ip-stat, tmsh
license

Displays the BIG-IP system software licensing information.

Module

sys

Syntax

Configure the license component within the sys module using the following syntax.

Display

show license
  options:
    detail

Description

You can use the license component to display detailed licensing and version information for the system, including the registration key, licensing dates, platform ID, suggested service check date, and the installed active modules.

Examples

Displays the system software licensing information:

show license

Displays the system software licensing information, including option modules, and active features:

show license detail

Options

For information about the options that you can use with the show command, see show, on page 3-39.

See also

show, tmsh
log

Displays various system log files.

Module

sys

Syntax

Configure the log component within the sys module using the following syntax.

Display

show log

show log [audit | daemon | gtm | kernel | ltm | mail | messages | security | tmm | \user | webui]

options:
  lines [integer]
  range [date range]

Description

You can use the log component to display various logs.

Examples

Displays a list of logs that you can view:

  show log

Displays the Global Traffic Manager™ log:

  show log gtm

Options

You can use these options with the log component:

  ◆ audit
    Displays a log of configuration changes.

  ◆ daemon
    Displays the UNIX® daemon logs.

  ◆ gtm
    Displays the Global Traffic Manager logs.
- **kernel**
  Displays Linux Kernel messages.

- **lines**
  Specifies how many lines of the log that you want the system to display at one time.

- **ltm**
  Displays Local Traffic Manager logs.

- **mail**
  Displays mail daemon logs.

- **messages**
  Displays application messages.

- **range**
  Specifies the date range of the log information that you want the system to display.

- **security**
  Displays security-related messages.

- **tmm**
  Displays Traffic Manager Microkernel logs.

- **user**
  Displays various user process logs.

- **webui**
  Displays Configuration utility logs.

### See also

- `show`, `tmsh`
log-rotate

Configures log rotation for the BIG-IP system.

Module

sys

Syntax

Configure the log-rotate component within the sys module using the following syntax.

Modify

modify log-rotate
options:
  common-backlogs [integer]
  common-include [string]
  description [string]
  include [string]
  mysql-include [string]
  syslog-include [string]
  tomcat-include [string]
  wa-include [string]
edit log-rotate
options:
  all-properties
  non-default-properties
  one-line

Display

list log-rotate
list log-rotate [option]
show running-config log-rotate
show running-config log-rotate [option]
options:
  all-properties
  non-default-properties
Description

You can configure the system to rotate the log files after a specified length of time. This helps to clear the hard drive of unneeded log files.

Examples

The system saves seven copies of the common log files:

```
modify log-rotate common-backlogs 7
```

Displays the configuration of the `log-rotate` component:

```
list log-rotate all-properties
```

Options

You can use these options with the `log-rotate` component:

- **common-backlogs**
  Specifies the number of logs that you want the system to save. Select a number from the valid range of 1 - 100. The default value is 24.

- **common-include**
  The default value is `none`.
  
  **Warning:** Do not use this option without assistance from the F5 Technical Support team. The system does not validate the commands issued using this option. If you use the common-include option incorrectly, you put the functionality of the system at risk.

- **description**
  User-defined description.

- **include**
  The default value is `none`.
  
  **Warning:** Do not use this option without assistance from the F5 Technical Support team. The system does not validate the commands issued using this option. If you use the include option incorrectly, you put the functionality of the system at risk.

- **syslog-include**
  The default value is `none`.
  
  **Warning:** Do not use this option without assistance from the F5 Technical Support team. The system does not validate the commands issued using this option. If you use the include option incorrectly, you put the functionality of the system at risk.

- **tomcat-include**
  The default value is `none`.
  
  **Warning:** Do not use this option without assistance from the F5 Technical Support team. The system does not validate the commands issued using this option. If you use the include option incorrectly, you put the functionality of the system at risk.
◆ wa-include
The default value is none.

Warning: Do not use this option without assistance from the F5 Technical Support team. The system does not validate the commands issued using this option. If you use the include option incorrectly, you put the functionality of the system at risk.

See also

edit, list, modify, show, tmsh
**mac-address**

Displays all MAC addresses currently associated with a configuration object on a BIG-IP system, including all dynamically-discovered MAC addresses.

**Module**

```
sys
```

**Syntax**

Display the IP addresses associated with a BIG-IP system configuration object using the syntax in the following section.

**Display**

```
show mac-address
```

**options:**

- `field-fmt`

**Description**

You can use the `mac-address` component to display the location on the BIG-IP system of the MAC addresses associated with a configuration object. The system displays the following information, which identifies the location of the MAC address in the configuration:

- **Entry**
  Displays the MAC address.
- **Component**
  Displays the type of component associated with the IP address, for example: `net interface`.
- **Object-ID**
  Displays the name of a configuration object associated with the MAC address, for example: `2.1`.
- **Property**
  When you specify the all-properties option, displays the name of the property that contains the IP address value. If the IP address is an object identifier the system displays `n/a`.

**Examples**

Displays all MAC addresses currently associated with a BIG-IP system configuration object:

```
show mac-address
```
Options

For information about the options that you can use with the `show` command, see `show`, on page 3-39.

See also

`show`, `tmsh`
management-ip

Configures the netmask for the management interface (MGMT).

Module

sys

Syntax

Configure the management-ip component within the sys module using the following syntax.

Create/modify

create management-ip [ip address/netmask]
create management-ip [ip address/prefixlen]
modify management-ip [ip address/prefixlen]
options:
    description

Display

list management-ip
show running-config management-ip
    options:
        all-properties
        one-line

Delete

delete management-ip [ip address/netmask]
delete management-ip [ip address/prefixlen]

Description

Specifies network settings for the management interface.
The management interface is available on all switch platforms and is designed for management purposes. You can access the browser-based Configuration utility and command line configuration utility through the management port. You cannot use the management interface in traffic management VLANs. You can configure only one IP address on the management interface.
After you make any changes using the management-ip component, issue the following command sequence to save the changes to the bigip_base.conf file: save base-config.

Examples

Creates the IP address 10.2.3.4 on the management interface:
create management-ip 10.2.3.4/255.255.0.0

Creates the IP address 10.2.3.4 on the management interface:
create management-ip 10.2.3.4/16

Options

You can use these options with the management-ip command:

- [ip address/netmask]
  Specifies the IPv4 address and netmask.

- [ip address/prefixlen]
  Specifies the IPv6 address and prefix length.

- description
  User-defined description.

See also

create, delete, list, modify, save, show, sys management-route, tmsh
management-route

Configures route settings for the management interface (MGMT).

Module

sys

Syntax

Configure the management-route component within the sys module using the following syntax.

Create/Modify

create management-route [name | default | default-inet6]
modify management-route [name | default | default-inet6]
  options:
    description [string]
    gateway [ip address]
    mtu [number]
    network [ip address/netmask]
edit management-route [ [ [name | default | default-inet6] | [glob] | [regex] ] ... ]
  options:
    all-properties

Display

list management-route
list management-route [ [ [name | default | default-inet6]
  | [glob] | [regex] ] ... ]
show running-config management-route
show running-config management-route [ [ [name | default
  | default-inet6] | [glob] | [regex] ] ... ]
  options:
    all-properties
    one-line

Delete

delete management-route [name]
Description

Specifies route settings for the management interface. You must configure a route on the management interface if you want to access the management network on the BIG-IP system by connecting from another network.

The management interface is available on all switch platforms and is designed for management purposes. You can access the browser-based Configuration utility and command line configuration utility through the management port. You cannot use the management interface in traffic management VLANs.

Examples

Sets the management interface default gateway IP address to 10.10.10.254:

create management-route default gateway 10.10.10.254

Creates a management route named myMgmtRoute for the subnet 10.10.10.0/24 whose gateway IP address is 10.10.10.254:

create management-route myMgmtRoute network 10.10.10.0/24 gateway 10.10.10.254

Changes the management interface to subnet 10.10.10.0/24 and the gateway to 172.24.74.62:

modify management-route 10.10.10.0/24 gateway 172.24.74.62

Options

You can use these options with the management-route component:

◆ default
  Indicates that the system forwards packets to the destination through the default IP address and netmask, 0.0.0.0 0.0.0.0.

◆ default-inet6
  Indicates that the system forwards packets to the destination through the default version 6.0 IP address and netmask.

◆ description
  User-defined description.

◆ glob
  Displays the items that match the glob expression. For a description of glob expression syntax, see the glob man page.

◆ [ip address/netmask]
  Specifies the IP address and netmask through which the system forwards packets to the destination. You can use either of these formats: 0.0.0.0/0 or 0.0.0.0 0.0.0.0.

◆ gateway
  Indicates that the system forwards packets to the destination through the gateway with the specified IP address.
◆ **mtu**
  Specifies the maximum transmission unit (MTU) for the management interface. The value of the MTU is the largest size that the BIG-IP system can accept for an IP datagram passing through the management interface.

◆ **network**
  The subnet and netmask to be used for the route. This is an optional field; if empty the name should be of the form [ip address/netmask].

◆ **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. For a description of regular expression syntax, see the **regex** man page.

See also

create, delete, edit, glob, list, modify, regex, show, sys management-ip, tmsh
mcp-state

Displays information about the mcpd daemon.

Module

sys

Syntax

Use the mcp-state component within the sys module to display information about the mcpd daemon using the following syntax.

Display

show mcp-state
  options:
    field-fmt

Description

You can use the mcp-state component to display the current state of the mcpd daemon.

Examples

Displays, in a table, information about the state of the mcpd daemon:
show mcp-state

Displays, in field format, information about the state of the mcpd daemon:
show mcp-state field-fmt

Options

For information about the options that you can use with the show command, see show, on page 3-39.

See also

show, tmsh
memory

Displays system memory information and statistics.

Module

sys

Syntax

Display statistics for the memory component within the sys module using the following syntax.

Display

```
show memory
options:
   (default | gig | global | kil | meg | raw)
   global
```

Description

You can use the memory component to display information about the system memory.

Examples

Displays memory statistics in gigabytes:
```
show memory gig
```
Displays raw memory statistics:
```
show memory raw
```

Options

For information about the options that you can use with the show command, see show, on page 3-39.

See also

```
show, tmsh
```
**ntp**

Configures the Network Time Protocol (NTP) daemon for the BIG-IP system.

**Module**

sys

**Syntax**

Configure the **ntp** component within the **sys** module using the following syntax.

**Modify**

```plaintext
modify ntp
  options:
    description [string]
    include [string]
    restrict [add | delete | replace-all-with] {
      [string] {
        address [IP address]
        default-entry [enabled | disable]
        description [string]
        ignore [enabled | disable]
        kod [enabled | disable]
        limited [enabled | disable]
        low-priority-trap [enabled | disable]
        mask [IP address]
        no-modify [enabled | disable]
        non-ntp-port [enabled | disable]
        no-peer [enabled | disable]
        no-query [enabled | disable]
        no-serve-packets [enabled | disable]
        no-trap [enabled | disable]
        no-trust [enabled | disable]
        ntp-port [enabled | disable]
        version [enabled | disable]
      }
    }
  restrict none
  servers [add | delete | replace-all-with] {
    [hostname | IP address] ...
  }
```


servers none
timezone [string]

edit ntp
options:
  all-properties
  non-default-properties

Display
list ntp
list ntp [option]
show running-config ntp
show running-config ntp [option]
  options:
    all-properties
    non-default-properties
    one-line

Description

You can use the ntp component to configure the NTP servers for the system.

Examples

Adds the NTP server with the IP address, 192.168.1.245, to the system:
modify ntp servers add {192.168.1.245}

Replaces the existing list of NTP servers with a single host, time.f5net.com:
modify ntp servers replace-all-with {time.f5net.com}

Sets the system time to Pacific Standard Time:
modify ntp timezone "America/Los_Angeles"

Adds a default restriction denying all packets:
modify ntp restrict add { basicrestrict { default-entry enable ignore enable } }

Options

You can use these options with the ntp component:

◆ description
  User-defined description.
Warning: Do not use this option without assistance from the F5 Technical Support team. The system does not validate the commands issued using the include option. If you use this option incorrectly, you put the functionality of the system at risk.

servers
Configures NTP servers for the BIG-IP system.

timezone
Specifies the time zone that you want to use for the system time.

restrict
Specifies a set of access restrictions.

- address
  The address for the entry. See also, the mask option. The default value is 0.0.0.0.

- default-entry
  Specifies whether the entry is the default entry. The default value is disabled.

- description
  User-defined description.

- ignore
  Specifies whether all packets will be ignored. The default value is disabled.

- kod
  Specifies whether a kod (kiss of death) packet will be sent when an access violation occurs. The default value is disabled.

- limited
  Specifies whether service will be denied if packet spacing limits are violated. The default value is disabled.

- low-priority-trap
  Specifies whether lower priority traps will be overridden by normal priority traps. The default value is disabled.

- mask
  The mask for the entry. See also, the address option. The default value is 0.0.0.0.

- no-modify
  Specifies whether ntpq and ntpdc queries that attempt to modify the server are allowed. The default value is disabled.

- non-ntp-port
  When enabled, the restrict entry will be matched only if the source port is not the standard NTP UDP port (123). The default value is disabled.

- no-peer
  Specifies whether packets will be denied if they mobilize a new association. The default value is disabled.
- **no-query**
  Specifies whether `ntpq` and `ntpd` queries will be denied. The default value is `disabled`.

- **no-serve-packets**
  Specifies whether all queries except `ntpq` and `ntpd` will be denied. The default value is `disabled`.

- **no-trap**
  Specifies whether to decline the `mode 6` control message trap service to matching hosts. The default value is `disabled`.

- **no-trust**
  Specifies whether to reject packets that are not cryptographically authenticated. The default value is `disabled`.

- **ntp-port**
  When enabled, the restrict entry will be matched only if the source port is the standard NTP UDP port (123). The default value is `disabled`.

- **version**
  Specifies whether packets will be rejected if they do not match the local NTP version. The default value is `disabled`.

### See also

`edit`, `list`, `modify`, `show`, `tmsh`
**proc-info**

Displays CPU and memory usage for each process.

**Module**

sys

**Syntax**

Display proc-info component within the sys module using the syntax in the following section.

**Display**

```
show proc-info
show proc-info process_name
```

```
options:
   (default | field-fmt | all | kil | meg | gig | raw | exa | peta | tera | zetta | yotta)
```

**Description**

show proc-info displays CPU and memory usage for each process and the process associated module name. This can be used to debug which process or module uses more resource.

**Options**

For information about the options that you can use with the show command, see show, on page 3-39.

**See also**

show, tmsh
provision

Configures provisioning on the BIG-IP system.

Module

sys

Syntax

Configure the provision component within the sys module using the following syntax.

Modify

modify provision

modify provision [ [all] | [apm | asm | em | gtm | lc | ltm | psm | wam | wom | woml] ]

options:
  cpu-ratio [integer]
  disk-ratio [integer]
  level [custom | dedicated | minimum | nominal | none]
  memory-ratio [integer]

edit provision

  [ [ [apm | asm | em | gtm | lc | ltm | psm | wam | wom | woml] |
    [glob] | [regex] ] ... ]

options:
  all-properties
  non-default-properties

Display

list provision

list provision

  [ [apm | asm | em | gtm | lc | ltm | psm | wam | wom | woml] |
    [glob] | [regex] ] ... ]

show running-config provision

show running-config provision

  [ [apm | asm | em | gtm | lc | ltm | psm | wam | wom | woml] |
    [glob] | [regex] ] ... ]

options:
  all-properties
  non-default-properties
  one-line
Description

You can use the provision component to modify the allocation of resources to the licensed modules on your system.

Examples

Provisions the minimum amount of resources for the BIG-IP Application Security Manager ™:

```
modify provision asm level minimum
```

Displays the current provisioning of the system:

```
list provision
```

Creates a transaction to modify the provisioning of a unit, to provision Local Traffic Manager at the minimum level and the Global Traffic Manager at the nominal level:

1. create transaction
2. modify /sys provision ltm level minimum
3. modify /sys provision gtm level nominal
4. submit transaction

Creates a transaction to modify the provisioning of a unit on which Local Traffic Manager is currently provisioned at the nominal level, to dedicate all of the unit’s resources to the Global Traffic Manager:

1. create transaction
2. modify /sys provision ltm level none
3. modify /sys provision gtm level dedicated
4. submit transaction

Options

You can use the following options with the provision component:

- **all**
  Indicates that you are provisioning all of the available modules.

- **apm**
  Indicates that you are provisioning the BIG-IP Access Policy Manager. When Access Policy Manager is provisioned the tmsh module apm is enabled.

- **asm**
  Indicates that you are provisioning the BIG-IP Application Security Manager.
◆ **cpu-ratio**
Use this option only when the **level** option is set to **custom**. F5 Networks recommends that you do not modify this option. The default value is **none**.

◆ **disk-ratio**
Use this option only when the **level** option is set to **custom**. F5 Networks recommends that you do not modify this option. The default value is **none**.

◆ **glob**
Displays the items that match the **glob** expression. For a description of **glob** expression syntax, see the **glob** man page.

◆ **em**
Indicates that you are provisioning the BIG-IP Enterprise Manager™.

◆ **gtm**
Indicates that you are provisioning the BIG-IP Global Traffic Manager. When Global Traffic Manager is provisioned, the **tmsh** module **gtm** is enabled.

◆ **lc**
Indicates that you are provisioning the BIG-IP Link Controller™ system. When **lc** is provisioned, the **tmsh** module **gtm** is enabled.

◆ **level**
Specifies the level of resources that you want to provision for a module. The options are:

  • **custom**
    F5 Networks recommends that you do not specify this level.

  • **dedicated**
    All resources are dedicated to the module you are provisioning. For all other modules, the **level** option must be set to **none**.

  • **minimum**
    Provisions the minimum amount of resources for the module you are provisioning.

  • **nominal**
    Shares all of the available resources equally among all of the modules that are licensed on the unit.

  • **none**
    Does not provision resources for this module.

◆ **ltm**
Indicates that you are provisioning the BIG-IP Local Traffic Manager.

◆ **memory-ratio**
Use this option only when the **level** option is set to **custom**. F5 Networks recommends that you do not modify this option. The default value is **none**.

◆ **psm**
Indicates that you are provisioning the BIG-IP Protocol Security Module™.
◆ **regex**
Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. For a description of regular expression syntax, see the `regex` man page.

◆ **wam**
Indicates that you are provisioning the BIG-IP WebAccelerator Module™. When WebAccelerator is provisioned, the `tmsh` module `wam` is enabled.

◆ **wom**
Indicates that you are provisioning the BIG-IP WAN Optimization Manager™. When WAN Optimization Manager is provisioned, the `tmsh` module `wom` is enabled.

◆ **woml**
Indicates that you are provisioning the BIG-IP WAN Optimization Manager Lite. When WAN Optimization Manager Lite is provisioned, the `tmsh` module `wom` is enabled.

---

**See also**

`edit`, `glob`, `list modify`, `regex`, `show`, `tmsh`
pva-traffic

Displays and resets Packet Velocity® ASIC (PVA) traffic statistics for the system.

Module

sys

Syntax

Configure the pva-traffic component within the sys module using the following syntax.

Modify

reset-stats pva-traffic

Display

show pva-traffic

options:

(default | exa | gig | kil | meg | peta | raw | tera | yotta | zetta)

global

Description

You can use the pva-traffic component to display traffic statistics, including bits in and out, packets in and out, current, maximum, and total connections, and other miscellaneous statistics.

◆ Note

The BIG-IP system has one PVA accelerator; however, when you run the show pva-traffic command, the system displays a PVA statistics entry for each Traffic Management Microkernel (TMM).

Examples

Displays PVA traffic statistics for the system:

show pva-traffic

Displays PVA traffic statistics for the system in raw data:

show pva-traffic raw
Options

For information about the options that you can use with the show command, see show, on page 3-39.

For information about the reset-stats command, see reset-stats, on page 3-31.

See also

reset-stats, show, sys tmm-traffic, tmsh
scriptd

Configures the scriptd daemon

Module

sys

Syntax

Configure the scriptd component within the sys module using the following syntax.

Modify

modify scriptd

options:
  log-level [alert | crit | debug | emerg | err | info | notice | warn]
  max-script-run-time [seconds]

Display

list scriptd
show running-config scriptd

options:
  all-properties

Description

You can use the scriptd component to configure the scriptd daemon. The scriptd daemon runs application template implementation scripts when an application service is created or updated (see sys application template and sys application service).

Examples

Displays scriptd configuration:

list scriptd

Updates the maximum time, in seconds, that a script is allowed to run:

restart service mcpd
Options

You can use the following options with the `scriptd` component:

- **log-level**
  Specifies the syslog level at which `scriptd` will generate log messages.

- **max-script-run-time**
  Specifies, in seconds, the maximum amount of time that a script is allowed to run before `scriptd` will kill the script. The default value is 300. The minimum value is 5.

See also

`list`, `modify`, `restart`, `show`, `start`, `stop`, `tmsh`
service

Manages services on the BIG-IP system.

Module

sys

Syntax

Configure the service component within the sys module using the following syntax.

Modify

modify service [name]
   options:
   [add | disable | enable | reinit | remove]
restart service [name]
start service [name]
stop service [name]
   options:
   force

Display

list service
list service [name]
show running-config service
show running-config service [name]
   options:
   all-properties
show service
   options:
   memstat

Description

You can use the service component to add, disable or enable, start, stop, restart, reinitialize, remove, or display information about a service.
Examples

Displays information about all services that are available on the system:

```
list service
```

Restarts the `mcpd` daemon:

```
restart service mcpd
```

Options

You can use the following options with the `service` component:

- **add**
  Adds the specified service.

- **disable**
  Disables the specified service.

- **enable**
  Enables the specified service.

- **memstat**
  Displays memory usage statistics for the specified service.

- **reinit**
  Reinitializes the specified service.

- **remove**
  Removes the specified service.

See also

```
list, modify, restart, show, start, stop, tmsh
```
smtp-server

Configure the SMTP server connection.

Module

sys

Syntax

Create or modify an SMTP server access configuration using the syntax in the following sections.

Modify

modify smtp-server [name]
create smtp-server [name]

options:
  [authentication-enabled | authentication-disabled]
  encrypted-connection [none | tls | ssl]
  local-host-name [string]
  smtp-server-host-name [string]
  smtp-server-port [integer]
  from-address [string]
  username [string]
  password [string]

Display

list smtp-server
show running-config smtp-server

options:
  all-properties

Description

You can use the smtp-server component to configure an SMTP server connection.

Examples

Displays the SMTP configuration:

list smtp-server
Chapter 39

Configures SMTP server connection with username=user and password=pass to be authenticated against the SMTP server mail.server.com. SSL encryption will be used for all communication with the SMTP server. Email messages will be sent out with the address example@f5.com in the "Reply-To" address.

modify smtp-server smtp1 authentication-enabled encrypted-connection ssl local-host-name example.f5.com from-address example@f5.com smtp-server-host-name mail.server.com username user password pass

Options

You can use the following options with the smtp-server component:

- **[authentication-enabled | authentication-disabled]**
  Enables or disables authentication against the configured SMTP server.

- **encrypted-connection**
  Specifies which type of encrypted connection the SMTP server requires in order to send mail. The default value is **none**.

- **local-host-name**
  Specifies the host name used in SMTP headers in the format of a fully qualified domain name. This setting does not refer to the BIG-IP system's Hostname, displayed at the top of the user interface screen.

- **smtp-server-host-name**
  Specifies the SMTP server host name in the format of a fully qualified domain name.

- **smtp-server-port**
  Specifies the SMTP port number. The default value is **25**.

- **from-address**
  Specifies the email address that the email is being sent from. This is the "Reply-to" address that the recipient sees.

- **username**
  Specifies the user name that the SMTP server requires when validating a user.

- **password**
  Specifies the password that the SMTP server requires when validating a user. This password is stored in an encrypted form.

See also

list, modify, restart, show, start, stop, tmsh
### Module

**sys**

### Syntax

Configure the **snmp** component within the **sys** module using the following syntax.

#### Modify

```bash
modify snmp
```

**options:**

- **agent-addresses [add | delete | replace-all-with] { ["agent:port"] ... }**
- **agent-addresses none**
- **agent-trap [enabled | disabled]**
- **allowed-addresses [add | delete | replace-all-with] { [IP address] }**
- **allowed-addresses none**
- **auth-trap [enabled | disabled]**
- **bigip-traps [enabled | disabled]**
- **communities [add | delete | modify | replace-all-with] { [name] {**
  - **options:**
    - **access [ro | rw]**
    - **community-name [string]**
    - **description [string]**
    - **ipv6 [enabled | disabled]**
    - **oid-subset [string]**
    - **source [default | [string]]**
  }
}
- **communities none**
- **description [string]**
- **disk-monitors [add | delete | modify | replace-all-with] { [name] {**
  - **options:**
    - **description [string]**
    - **minspace [integer]**
    - **minspace-type [percent | size]**
```
path [string]
)
}
disk-monitors none
include [string]

l2forward-vlan [all | add | delete | replace-all-with] { [VLAN name] ...
}
l2forward-vlan none
load-max1 [integer]
load-max5 [integer]
load-max15 [integer]

process-monitors [add | delete | modify | replace-all-with] {
[name] {
    options:
        process [string]
        min-processes [integer]
        max-processes [integer] | infinity
    }
}
process-monitors none
sys-contact [string]
sys-location [string]
sys-services [integer]
trap-community [string]
trap-source [IP address]

traps [add | delete | modify | replace-all-with] {
[name] {
    options:
        auth-password [string]
        auth-protocol [md5 | sha | none]
        community [string]
        description [string]
        engine-id [none | [number]]
        host [ [ip address] | [FQDN] | [protocol]:[ip address] ] | [[protocol]:[FQDN]]
        port [integer]
        privacy-password [string]
        privacy-protocol [aes | des | none]
        security-level [auth-no-privacy | auth-privacy | no-auth-no-privacy]
        security-name [string]
        version [1 | 2c | 3]
    }
}

traps none

users [add | delete | modify | replace-all-with] {
[user name] {
    options:
        access [ro | rw]
        auth-password [string]
auth-protocol [md5 | sha | none]
description [string]
oid-subset [string]
privacy-password [string]
privacy-protocol [aes | des | none]
security-level [auth-no-privacy | auth-privacy | no-auth-no-privacy]
version [1 | 2c | 3]
username [string]
}
}
users none
v1-traps [add | delete | modify | replace-all-with] }
[name] {
options:
  community [string]
description [string]
  host [ [ip address] | [FQDN] | [ [protocol]:[ip address] ] | [[protocol]:[FQDN]] ]
  port [integer]
}

v1-traps none
v2-traps [add | delete | modify | replace-all-with] }
[name] {
options:
  community [string]
description [string]
  host [ [ip address] | [FQDN] | [ [protocol]:[ip address] ] | [[protocol]:[FQDN]] ]
  port [integer]
}

v2-traps none
edit snmp
options:
  all-properties
  non-default-properties

Display

list snmp
list snmp [option]
show running-config snmp
show running-config snmp [option]
options:
  all-properties
  non-default-properties
  one-line
Description

You can use the `snmp` component to configure the `snmpd` daemon for the BIG-IP system.

**Important**

F5 Networks recommends that users of the Configuration utility exit the utility before changes are made to the system using the command sequence `tmsh sys snmp`. This is because making changes to the system using this command causes a restart of the `snmpd` daemon. Likewise, restarting the `snmpd` daemon creates the necessity for a restart of the Configuration utility.

Examples

Indicates that the person who administers the `snmpd` daemon for the system can be reached using the email address, admin@company.com:

```
modify snmp sys-contact admin@company.com
```

Indicates that the physical location of the system is the central office:

```
modify snmp sys-location "central office"
```

Disables agent traps:

```
modify snmp agent-trap disabled
```

Adds a range of SNMP clients to the `/etc/hosts.allow` file:

```
modify snmp allowed-addresses add {10.10.0.0/255.255.240.0}
```

Adds an SNMP version 1 trapsess, `tv1`, to the system. The destination IP address of `tv1` is 192.168.1.240, the port is 162, and the community that has access to `tv1` is `public`.

```
modify snmp traps add { tv1 { version 1 community public host 192.168.1.240 port 162 } }
```

Adds an SNMP version 2 trapsess, `tv2`, to the system. The destination IP address of `tv2` is 192.168.1.241, the port is 162, and the community that has access to `tv2` is `public`.

```
modify snmp traps add { tv2 { version 2c community public host 192.168.1.241 port 162} }
```

Adds an SNMP version 3 trapsess, `trap_v3_1`, with authentication capabilities to the system. The destination IP address of `trap_v3_1` is 192.168.1.242, the port is 162, the security level is the authentication without privacy, the security name is `mySecurityName`, the authentication protocol is MD5, and the authentication password is `myAuthPassword`.

```
modify snmp traps add { trap_v3_1 { version 3 host 192.168.1.242 port 162 security-level auth-no-privacy security-name mySecurityName auth-protocol md5 auth-password myAuthPassword } }
```
Adds an SNMP version 3 trapsink, trap_v3_2, with authentication and privacy capabilities to the system. The destination IP address of trap_v3_2 is 192.168.1.243, the port is 162, the security level is the authentication and privacy, the security name is mySecurityName, the authentication protocol is SHA, the authentication password is myAuthPassword, the privacy protocol is AES, and the privacy password is myPrivacyPassword.

modify snmp traps add { trap_v3_2 { version 3 host 192.168.1.243 port 162 security-level auth-privacy security-name mySecurityName auth-protocol sha auth-password myAuthPassword privacy-protocol aes privacy-password myPrivacyPassword } }

Adds an SNMP version 1 trapsink, ts, to the system. The destination IP address of ts is 10.20.5.11, the port is 162, and the community that has access to ts is public.

modify snmp v1-traps add { ts { community public host 10.20.5.11 port 162 } }

Adds an SNMP version 2 trap2sink, t2s, to the system. The destination IP address of t2s is 10.20.5.12, the port is 162, and the community that has access to t2s is public.

modify snmp v2-traps add { t2s { community public host 10.20.5.12 port 162 } }

Adds an SNMP version 3 user with the user name, myUser1, to the system. The access to the management information base (MIB) of myUser1 is read-only, the security level is the authentication without privacy, the authentication protocol is MD5, and the authentication password is myAuthPassword.

modify snmp users add { myUser1 { username myUser1 access ro security-level auth-no-privacy auth-protocol md5 auth-password myAuthPassword privacy-protocol none } }

Adds an SNMP version 3 user with the user name, myUser2, to the system. The access to the management information base (MIB) of myUser2 is read-only (by default) and restricted to every object below the 1.3.6.1.4.1.3375 object identifier in the MIB tree, the security level is the authentication without privacy, the authentication protocol is MD5, and the authentication password is myAuthPassword.

modify snmp users add { myUser2 { username myUser2 oid-subset .1.3.6.1.4.1.3375 auth-protocol md5 auth-password myAuthPassword privacy-protocol none } }

Adds an SNMP version 3 user with the user name, myUser3, to the system. The access to the management information base (MIB) of myUser3 is read-only, the security level is the authentication and privacy, the authentication protocol is SHA, the authentication password is myAuthPassword, the privacy protocol is DES, and the privacy password is myPrivacyPassword.

modify snmp users add { myUser3 { username myUser3 access ro security-level auth-privacy auth-protocol sha auth-password myAuthPassword privacy-protocol des privacy-password myPrivacyPassword } }

Adds an SNMP version 3 user with the user name, myUser4, to the system. The access to the management information base (MIB) of myUser4 is read-only without the authentication and privacy settings.

modify snmp users add { myUser4 { username myUser4 access ro security-level no-auth-no-privacy auth-protocol none privacy-protocol none } }
Creates a community specification named `community1` for the BIG-IP system. `community1` includes a community, named `mycommunity`, that provides read-only access to the host at `192.168.1.246`. This host cannot be an IPv6 address. The oid for this community is `5`.

```plaintext
modify snmp communities add { community1 { community-name mycommunity access ro source 192.168.1.246 oid-subset 5 ipv6 disabled } }
```

Replaces the default community specification for the BIG-IP system. Using this command, the default community includes a community, named `public`, that provides read-only access to the default host. The oid for this community is `1`:

```plaintext
modify snmp communities add { new-name { community-name public source default oid-subset 1 access ro } }
```

Deletes the community named `mycommunity`:

```plaintext
modify snmp communities delete { mycommunity }
```

Disables monitoring of `snmpd` load average on the BIG-IP system:

```plaintext
modify snmp load-max1 0 load-max5 0 load-max15 0
```

**Options**

You can use the following options with the `snmp` component:

- **agent-addresses**
  Indicates that the SNMP agent is to listen on the specified address. Do not change this setting without fully understanding the impact of the change.

- **agent-trap**
  Specifies, when `enabled`, that the `snmpd` daemon sends traps, for example, start and stop traps. The default value is `enabled`.

- **allowed-addresses**
  Configures the IP addresses of the SNMP clients from which the `snmpd` daemon accepts requests. An SNMP client is a system that runs the SNMP manager software for the purpose of remotely managing the BIG-IP system. The default value is `127`.

- **auth-trap**
  Specifies, when `enabled`, that the `snmpd` daemon generates authentication failure traps. The default value is `disabled`.

- **bigip-traps**
  Specifies, when `enabled`, that the BIG-IP system sends device warning traps to the trap destinations. The default value is `enabled`.

- **community**
  Configures a community for the `snmpd` daemon. You must include a community key, and you must enclose the attributes in braces. The options are additive and include:
• **access**
  Specifies the community access level to the MIB. The access options are **ro** (read-only) or **rw** (read-write). The default value is **ro**.

• **community name**
  Specifies the name of the community that you are configuring for the **snmpd** daemon. This option is required. The default value is **public**.

• **description**
  User-defined description.

• **ipv6**
  Enables or disables IPv6 addresses for the community that you are configuring. The default value is **disabled**.

• **oid-subset**
  Restricts access by the community to every object below the specified object identifier (OID) for the record.

• **source**
  Specifies the source addresses with the specified community name that can access the management information base (MIB). The default value is **default**, which means allow any source address to access the MIB.

• **description**
  User-defined description.

• **disk-monitors**
  Checks the disks mounted at the specified path for available disk space.
  
The options are:

  • **description**
    User-defined description.

  • **minspace**
    Specifies the minimum disk space threshold in either kBs or percentage based on the value of the **minspace-type** option. If the available disk space is less than this amount, the associated entry in the 1.3.6.1.4.1.2021.9.1.100 MIB table is set to (1) and a descriptive error message is returned to queries of 1.3.6.1.4.1.2021.9.1.101.

  • **minspace-type**
    Specifies a minimum disk space measurement type of either size in kB, or percent. The value of the **minspace** option is based on the value of this option.

  • **path**
    Specifies the path to the disk that the system checks for disk space. This option is required.

• **include**
  **Warning:** Do not use this parameter without assistance from the F5 Technical Support team. The system does not validate the commands issued using the include parameter. If you use this parameter incorrectly, you put the functionality of the system at risk.
◆ l2forward-vlan
   Specifies the VLANs for which you want the snmpd daemon to expose Layer 2 forwarding information. Layer 2 forwarding is the means by which frames are exchanged directly between hosts, with no IP routing required. The default value is none.

   The options are:
   • all
     Specifies that the snmpd daemon exposes Layer 2 forwarding information for all VLANs.
     **Warning:** When you set this option to all, the system can create a very large table of statistics and potentially affect system performance.
   • none
     Indicates that this option is not set.
     **Important:** The default value is not the same as setting this option to the string “none,” which indicates that you do not want the snmpd daemon to expose Layer 2 forwarding for any VLAN.
   • VLAN name
     Specifies the names of the VLANs for which the snmpd daemon exposes Layer 2 forwarding information. The snmpd daemon overwrites the value of the sysL2ForwardAttrVlan object identifier (OID) with the specified VLAN names. Once you set this parameter, users cannot change the value of the sysL2ForwardAttrVlan OID using the SNMP set method.

◆ load-max1
   Specifies the maximum 1-minute load average of the machine. If the load exceeds this threshold, the associated entry in the 1.3.6.1.4.1.2021.10.1.100 MIB table is set to (1) and a descriptive error message is returned to queries of 1.3.6.1.4.1.2021.10.1.101.

   When you specify a 0 (zero) for all three of the load-max1, load-max5, and load-max15 options, the system does not monitor the load average.

◆ load-max5
   Specifies the maximum 5-minute load average of the machine. If the load exceeds this threshold, the associated entry in the 1.3.6.1.4.1.2021.10.1.100 MIB table is set to (1) and a descriptive error message is returned to queries of 1.3.6.1.4.1.2021.10.1.101.

   When you specify a 0 (zero) for all three of the load-max1, load-max5, and load-max15 options, the system does not monitor the load average.

◆ load-max15
   Specifies the maximum 15-minute load average of the machine. If the load exceeds this threshold, the associated entry in the 1.3.6.1.4.1.2021.10.1.100 MIB table is set to (1) and a descriptive error message is returned to queries of 1.3.6.1.4.1.2021.10.1.101.

   When you specify a 0 (zero) for all three of the load-max1, load-max5, and load-max15 options, the system does not monitor the load average.

◆ process-monitors
   Checks the machine to determine if the specified process is running. An error flag (1) and a description message are passed to the
1.3.6.1.4.1.2021.2.1.100 and 1.3.6.1.4.1.2021.2.1.101 MIB columns (respectively), if the specified program is not found in the process table as reported by `/bin/ps -e`.

F5 Networks recommends that you do not modify or delete system processes; however, you can add, modify, or delete user-defined processes.

The options are:

- **description**
  User-defined description.

- **max-processes**
  Specifies the maximum number of instances of the process that can run. The default value is 1. If you do not specify values for the **min-processes** and **max-processes** options, the **max-processes** option is 1 by default.

- **min-processes**
  Specifies the minimum number of instances of the process that can run. The default value is 1. If you do not specify a value for the **max-processes** option, and the **min-processes** option is not specified, the **min-processes** option is 0 (zero) by default.

- **process**
  Specifies the name of the monitored process. The maximum length for a process name is 16 characters. This option is required.

- **sys-contact**
  Specifies the name of the person who administers the **snmpd** daemon for this system. The default value is “Customer Name@admin@customer.com”.

  **Note:** If you enter a string that contains spaces, you must enclose the string in quotation marks and use backslashes to escape the quotation marks (for example: "John Doe").

- **sys-location**
  Describes this system’s physical location. The default value is **Network Closet 1**.

  **Note:** If you enter a string that contains spaces, you must enclose the string in quotation marks and use backslashes to escape the quotation marks (for example: "Engineering Lab").

- **sys-services**
  Specifies the value of the **system.sysServices.0** object. The default value is 78.

- **trap-community**
  Specifies the community name for the trap destination. The default value is **public**.

- **traps**
  Configures the SNMP version 1, version 2, or version 3 trap destination. You must include a trapsess key, and you must enclose the attributes in braces. The options are additive and include:
• **auth-password**
  Specifies the authentication password, which must be at least eight characters long. This option is valid only for SNMP version 3. If you enter an authentication password, the value of the **auth-protocol** option cannot be set to **none**.

• **auth-protocol**
  Specifies the authentication method to use to deliver the trap message. The default value is **none**. You can specify the following authentication methods:
  - **md5**
    The system uses the message digest algorithm (MD5) to authenticate the trap message. This value is valid only for SNMP version 3.
  - **none**
    The system does not authenticate the trap message. If you use this value, you cannot use the **auth-password** option. This option is invalid for SNMP version 3.
  - **sha**
    The system uses the secure hash algorithm (SHA) to authenticate the trap message. This option is valid only for SNMP version 3.

• **community**
  Specifies a community that has access to the trap message. This option is required only for SNMP version 1 and 2.

• **description**
  User-defined description.

• **engine-id**
  Specifies the unique authoritative security engine ID for SNMP version 3. This option is valid only for SNMP version 3. The default value is **none**. You can find the engine ID generated by the SNMP agent in `/config/net-snmp/snmpd.conf` on the BIG-IP system. Note that it is identified as `oldEngineID` in this file.

• **host**
  Specifies the trap destination that you are configuring, the IP address, FQDN, or either of these with an embedded protocol, for example `tcp:10.10.10.1` or `tcp:www.f5.com`. You must configure the DNS server on the BIG-IP system. You can use the `sys dns` command to do this. This option is required.

• **port**
  Specifies the port for the trap destination that you are configuring. The default value is **162**.

• **privacy-password**
  Specifies the privacy password, which must be at least eight characters long. This option is valid only for SNMP version 3. If you enter a privacy password, the value of the **privacy-protocol** option cannot be set to **none**.

• **privacy-protocol**
  Specifies the encryption/privacy method to use to deliver the trap message. The default value is **none**.
You can specify the following privacy methods:

- **aes**
  The system encrypts the trap message using Advanced Encryption Standard (AES). This value is valid only for SNMP version 3.

- **des**
  The system encrypts the trap message using the Data Encryption Standard (DES). This value is valid only for SNMP version 3.

- **none**
  The system does not encrypt the trap message. If you use this value, you cannot use the `privacy-password` option.

- **security-level**
  Specifies the security level to use to deliver the trap message. The default value is **no-auth-no-privacy**. You can specify the following security levels:

  - **no-auth-no-privacy**
    Provides no authentication and no encryption for the trap message. This value is invalid for SNMP version 3.

  - **auth-no-privacy**
    Provides authentication without encryption for the trap message. Specifies to use the value of the `auth-protocol` option, but not the value of the `privacy-protocol` option. Note that if you use this option, the value of the `auth-protocol` option cannot be set to **none**, and you must configure a value for the `auth-password` option. This value is valid only for SNMP version 3.

  - **auth-privacy**
    Provides authentication and encryption for the trap message. Specifies to use the value of the `auth-protocol` and `privacy-protocol` options. Note that if you use this option, the value of the `auth-protocol` and `privacy-protocol` options cannot be set to **none**, and you must configure a value for the `auth-password` and `privacy-password` options. This option is valid only for SNMP version 3.

- **security-name**
  Specifies the security name the system uses to handle SNMP version 3 trap messages. The default value is **none**. This option is required for SNMP version 3.

- **version**
  Specifies the security model to use. The options are **1** (version 1), **2c** (version 2), or **3** (version 3). The default value is **2c**.

- **trap-source**
  Specifies the source of the SNMP trap. The default value is **none**.

- **users**
  Configures the users for which you are setting SNMP version 3 access. You must include a user key, and you must enclose the attributes in braces. The options are additive and include:
• **access**
  Specifies the user access level to the management information base (MIB.) The access options are **ro** (read-only) or **rw** (read-write). The default value is **ro**.

• **auth-password**
  Specifies the authentication password, which must be at least eight characters long. If you enter an authentication password, the value of the **auth-protocol** option cannot be set to **none**.

• **auth-protocol**
  Specifies the authentication method to use to deliver the SNMP message. This option is required. You can specify the following authentication methods:
  - **none**
    Specifies that the system does not authenticate the SNMP message. Note that if you use this value, you must set the **security-level** to **no-auth-no-privacy** and you cannot use the **auth-password** option.
  - **md5**
    Specifies that the system uses the message digest algorithm (MD5) to authenticate the SNMP message.
  - **sha**
    Specifies that the system uses the secure hash algorithm (SHA) to authenticate the SNMP message.

• **description**
  User-defined description.

• **oid-subset**
  Specifies to restrict access by the user to every object below the specified object identifier (OID).

• **privacy-password**
  Specifies the privacy password, which must be at least eight characters long. If you enter the privacy password, the value of the **privacy-protocol** option cannot be set to **none**.

• **privacy-protocol**
  Specifies the encryption/privacy method to use to deliver the SNMP message. This option is required. You can specify the following encryption methods:
  - **aes**
    The system encrypts the SNMP message using Advanced Encryption Standard (AES).
  - **des**
    The system encrypts the SNMP message using Data Encryption Standard (DES).
  - **none**
    The system does not encrypt the SNMP message. If you use this value, you cannot use the **privacy-password** option.
◆ security-level
  Specifies the security level to use to deliver the SNMP message. You can use the following security levels:
  * no-auth-no-privacy
    Provides no authentication and no encryption for the SNMP message.
  * auth-no-privacy
    Provides authentication without encryption for the SNMP message using the value of the auth-protocol option, but not the value of the privacy-protocol option. Note that if you use this option, the value of the auth-protocol option cannot be set to none, and you must configure a value for the auth-password option.
  * auth-privacy
    Provides authentication and encryption for the SNMP message using the value of the auth-protocol and privacy-protocol options. Note that if you use this option, the value of the auth-protocol and privacy-protocol options cannot be set to none, and you must configure a value for the auth-password and privacy-password options.

◆ username
  Specifies the name of the user who is using SNMP version 3 to access the management information base (MIB). This option is required.

◆ v1-traps
  Configures an SNMP version 1 trap destination. You must include a version 1 trapsink key, and you must enclose the attributes in braces. The options are additive and include:
  * community
    Specifies the community name for the trap destination that you are configuring. This option is required.
  * description
    User-defined description.
  * host
    Specifies the trap destination that you are configuring, the IP address, FQDN, or either of these with an embedded protocol, for example tcp:10.10.10.1 or tcp:www.f5.com. You must configure the DNS server on the BIG-IP system. You can use the sys dns command to do this. This option is required.
  * port
    Specifies the port for the trap destination that you are configuring. The default value is 162.

◆ v2-traps
  Configures an SNMP version 2 trap destination. You must include a version 2 trap2sink key, and you must enclose the attributes in braces. The options are additive and include:
  * community
    Specifies the community name for the trap destination that you are configuring. This option is required.
• **description**
  User-defined description.

• **host**
  Specifies the trap destination that you are configuring, the IP address, FQDN, or either of these with an embedded protocol, for example `tcp:10.10.10.1` or `tcp:www.f5.com`. You must configure the DNS server on the BIG-IP system. You can use the `sys dns` command to do this. This option is required.

• **port**
  Specifies the port for the trap destination that you are configuring. The default value is **162**.

**See also**

`edit, list modify, show, tmsh`
sshd

Configures the Secure Shell (SSH) daemon for the BIG-IP system.

Module

sys

Syntax

Configure the sshd component within the sys module using the syntax in the following sections.

Modify

modify sshd
  options:
  
  allow [add | delete | replace-all-with] ( [ [hostname] | [IP address] ] ... )
  allow none
  banner [disabled | enabled]
  banner-text [string]
  inactivity-timeout [integer]
  include [string]
  login [disabled | enabled]
  log-level [debug | debug1 | debug2 | debug3 | error | fatal | info | quiet | verbose]

edit sshd
  options:
  
  all-properties
  non-default-properties

Display

list sshd
list sshd [option]
show running-config sshd
show running-config sshd [option]
  options:
  
  all-properties
  non-default-properties
  one-line
Description

You can use the `sshd` component to configure a secure channel between the BIG-IP system and other devices.

F5 Networks recommends that users of the Configuration utility exit the utility before changes are made to the system using the `sshd` component. This is because making changes to the system using this component causes a restart of the `sshd` daemon. Likewise, restarting the `sshd` daemon creates the necessity for a restart of the Configuration utility.

Examples

Creates an initial range of IP addresses (192.168.0.0 with a netmask of 255.255.0.0) that are allowed to log in to the system:

```
modify sshd allow add {192.168.0.0/255.255.0.0}
```

Adds the IP address, 192.168.1.245, to the existing list of IP addresses that are allowed to log in to the system:

```
modify sshd allow add {192.168.1.245}
```

Enables SSH login to the system:

```
modify sshd login enabled
```

Sets an inactivity timeout of 60 minutes for SSH logins to the system:

```
modify sshd inactivity-timeout 3600
```

Sets the `sshd` message log level to ERROR:

```
modify sshd log-level error
```

Creates a banner that displays when a user attempts to log in to a system using SSH:

```
modify sshd banner enabled banner-text "NOTICE: Improper use of this computer may result in prosecution!"
```

**Note**

You must enclose the banner text in double quotation marks, and then type single quotation marks outside the double quotation marks. You can also use the backslash character to escape each quotation mark as well as any other special characters that the system might process, for example, exclamation point (!).
Options

You can use the following options with the `sshd` component:

- **allow**
  Configures servers in the `/etc/hosts.allow` file. The default value is `all`.  
  *Warning:* Using the value `none` resets the `sshd` daemon to allow all servers access to the system. F5 Networks recommends that you do not use the value `none` with the `sshd` component.

- **banner**
  Enables or disables the display of the banner text field when a user logs in to the system using SSH. The default value is `disabled`.

- **banner-text**
  When the `banner` option is `enabled`, specifies the text to include in the banner that displays when a user attempts to log on to the system.

- **inactivity-timeout**
  Specifies the number of seconds before inactivity causes an SSH session to log out. The default value is 0 (zero) seconds, which indicates that inactivity timeout is disabled.

- **include**
  *Warning:* Do not use this option without assistance from the F5 Technical Support team. The system does not validate the commands issued using the `include` option. If you use this option incorrectly, you put the functionality of the system at risk.

- **login**
  Enables or disables SSH logins to the system. The default value is `enabled`.

- **log-level**
  Specifies the minimum `sshd` message level to include in the system log. The possible values are:
  - `debug - debug3`
    Indicates that the minimum `sshd` message level that the system logs is the specified debugging level of messages.
  - `error`
    Indicates that the minimum `sshd` message level that the system logs is error.
  - `fatal`
    Indicates that the minimum `sshd` message level that the system logs is fatal.
  - `info`
    Indicates that the minimum `sshd` message level that the system logs is informational.
  - `quiet`
    Indicates that the system does not log `sshd` messages.
  - `verbose`
    Indicates that the system logs all `sshd` messages.
See also

edit, list, modify, show, tmsh
state-mirroring

Configures connection mirroring for a BIG-IP system that is part of a high availability system.

Module

sys

Syntax

Configure the state-mirroring component within the sys module using the syntax in the following sections.

Modify

modify state-mirroring
options:
addr [ip address]
peer-addr [ip address]
secondary-addr [ip address]
secondary-peer-addr [ip address]
state [enabled | disabled]
edit state-mirroring
options:
all-properties
non-default-properties
one-line

Display

list state-mirroring
list state-mirroring [option]
show running-config state-mirroring
show running-config state-mirroring [option]
options:
all-properties
non-default-properties
Chapter 39

Description

You can use the **state-mirroring** component to configure connection mirroring on a system that is part of a high availability system.

Connection mirroring is the process of duplicating connections from the active system to the standby system. Enabling this setting ensures a higher level of connection reliability, but it can also have an impact on system performance.

Examples

Enables and configures connection mirroring for a high availability system in which one BIG-IP system has an IP address of **192.168.10.10**, and its peer has an IP address of **192.168.10.20**:

```
modify state-mirroring state enabled addr 192.168.10.10 peer-addr 192.168.10.20
```

Re-enables connection mirroring for a system for which connection mirroring was **disabled**:

```
modify state-mirroring state enabled
```

Options

You can use the following options with the **state-mirroring** component:

- **addr**
  Specifies the primary self IP address on this unit to which the peer unit in this redundant system configuration mirrors its connections. The default value is `::`.

- **peer-addr**
  Specifies the primary self IP address on the peer unit to which this unit mirrors its connections. The default value is `::`.

- **secondary-addr**
  Specifies another self IP address on this unit to which the peer unit mirrors its connections when the primary address is unavailable. The default value is `::`.

- **secondary-peer-addr**
  Specifies another self IP address on the peer unit to which this unit mirrors its connections when the primary peer address is unavailable. The default value is `::`.

- **state**
  Enables or disables connection mirroring. The default value is **enabled**.

See also

`edit, list, modify, show, tmsh`
**sync-sys-files**

Syncs a pre-defined set of system files from a device.

**Module**

sys

**Syntax**

Sync a pre-defined set of system files within the sys module using the syntax in the following sections.

**Run**

```sh
code
run sync-sys-files
options:
  from [ip address]
```

**Display**

```sh
code
show sync-sys-files
```

**Description**

You can use the `sync-sys-files` component to sync system files listed in `/usr/share/defaults/sys_files.spec` from a remote device. Only admins can exercise this command.

**Examples**

Syncs the list of files (as given in `/usr/share/defaults/sys_file.spec`) from the IP address `172.27.34.182`.

```sh
code
run sync-sys-files from 172.27.34.182
```

Shows the last sync time and the source device from where the files are synced.

```sh
code
show sync-sys-files
```
Options

You can use the following options with the `sync-sys-files` component:

- **from**
  Specifies the IP address used for configuration synchronization on the device from which you want to sync system files.
syslog

Configures the BIG-IP system log.

Module

sys

Syntax

Configure the syslog component within the sys module using the syntax in the following sections.

Modify

modify syslog

options:
- auth-priv-from [alert | crit | debug | emerg | err | info | notice | warning]
- auth-priv-to [alert | crit | debug | emerg | err | info | notice | warning]
- cron-from [alert | crit | debug | emerg | err | info | notice | warning]
- cron-to [alert | crit | debug | emerg | err | info | notice | warning]
- daemon-from [alert | crit | debug | emerg | err | info | notice | warning]
- daemon-to [alert | crit | debug | emerg | err | info | notice | warning]
- description [string]
- include [string]
- iso-date [enabled | disabled]
- kern-from [alert | crit | debug | emerg | err | info | notice | warning]
- kern-to [alert | crit | debug | emerg | err | info | notice | warning]
- mail-from [alert | crit | debug | emerg | err | info | notice | warning]
- mail-to [alert | crit | debug | emerg | err | info | notice | warning]
- messages-from [alert | crit | debug | emerg | err | info | notice | warning]
- messages-to [alert | crit | debug | emerg | err | info | notice | warning]
- remote-servers { add | delete | modify | replace-all-with } {
  [name] {
    options:
    - host [hostname]
    - local-ip [IP address]
    - remote-port [port number]
  }
}
- remote-servers none
- user-log-from [alert | crit | debug | emerg | err | info | notice | warning]
- user-log-to [alert | crit | debug | emerg | err | info | notice | warning]
Chapter 39

```
edit syslog
options:
  all-properties
  non-default-properties

Display

list syslog
list syslog [option]
show running-config syslog
show running-config syslog [option]
  options:
    all-properties
    non-default-properties
    one-line

Description

You can use the syslog component to configure the system log.

Examples

Resets the lowest level of messages about user authentication that are included in the system log to messages with a level of warning, error, critical, alert, and emergency:

```
modify syslog auth-priv-from warning
```

Resets the highest level of messages about user authentication that are included in the system log to messages with a level of warning, error, critical, alert, and emergency:

```
modify syslog auth-priv-to warning
```

Options

You can use the following options with the syslog component:

- **item auth-priv-from**
  Specifies the lowest level of messages about user authentication to include in the system log. The default value is notice.

- **auth-priv-to**
  Specifies the highest level of messages about user authentication to include in the system log. The default value is emerg.

- **cron-from**
  Specifies the lowest level of messages about time-based scheduling to include in the system log. The default value is warning.
- **cron-to**
  Specifies the highest level of messages about time-based scheduling to include in the system log. The default value is `emerg`.

- **daemon-from**
  Specifies the lowest level of messages about daemon performance to include in the system log. The default value is `notice`.

- **daemon-to**
  Specifies the highest level of messages about daemon performance to include in the system log. The default value is `emerg`.

- **host**
  Specifies the IP address of a remote server to which the syslog-ng utility sends messages. The default value is `none`.

- **include**
  **Warning**: Do not use this option without assistance from the F5 Technical Support team. The system does not validate the commands issued using the include options. If you use this option incorrectly, you put the functionality of the system at risk.

- **kern-from**
  Specifies the lowest level of kern messages to include in the system log. The default value is `notice`.

- **kern-to**
  Specifies the highest level of kern messages to include in the system log. The default value is `emerg`.

- **local-ip**
  Specifies the IP address of the interface that syslog binds with to log messages to a remote host. For example, if you want syslog to log messages to a remote host that is connected to a VLAN, you set this parameter to the self IP address of the VLAN.

- **mail-from**
  Specifies the lowest level of mail log messages to include in the system log. The default value is `notice`.

- **mail-to**
  Specifies the highest level of mail log messages to include in the system log. The default value is `emerg`.

- **messages-from**
  Specifies the lowest level of messages about user authentication to include in the system log. The default value is `notice`.

- **messages-to**
  Specifies the highest level of system messages to include in the system log. The default value is `warning`.

- **remote-port**
  Specifies the port number of a remote server to which syslog sends messages. The default value is 514.

- **remote-servers**
  Configures the remote servers, identified by IP address, to which syslog sends messages. The default value is `none`. 
◆ user-log-from
   Specifies the lowest level of user account messages to include in the system log. The default value is notice.

◆ user-log-to
   Specifies the highest level of user account messages to include in the system log. The default value is emerg.

See also

edit, list, modify, show, tmsh
tmm-info

Displays information about the Traffic Management Microkernel (tmm) daemon.

Module

sys

Syntax

Display statistics for the tmm-info component within the sys module using the following syntax.

Display

show tmm-info

options:

(default | exa | gig | kil | meg | peta | raw | tera | yotta | zetta)

global

Description

You can use the tmm-info component to display information about the tmm daemon. The purpose of this daemon is to direct all application traffic passing through the BIG-IP system.

Options

For information about the options that you can use with the show command, see show, on page 3-39.

See also

show, sys tmm-traffic, tmsh
**tmm-traffic**

Displays Traffic Management Microkernel (TMM) statistics.

**Module**

sys

**Syntax**

Configure the tmm-traffic component within the sys module using the following syntax.

**Modify**

reset-stats tmm-traffic

**Display**

show tmm-traffic

options:

- (default | exa | gig | kil | meg | peta | raw | tera | yotta | zetta)
- global

**Description**

You can use the tmm-traffic component to display TMM traffic statistics, including errors and redirected connections. The purpose of this daemon is to direct all application traffic passing through the BIG-IP system.

**Options**

For information about the options that you can use with the show command, see show, on page 3-39.

For information about the reset-stats command, see reset-stats, on page 3-31.

**See also**

reset-stats, show, sys pva-traffic, sys tmm-info, tmsh
traffic

Displays or resets traffic statistics for the system.

Module

sys

Syntax

Configure the traffic component within the sys module using the following syntax.

Modify

reset-stats traffic

Display

traffic show

options:
(default | exa | gig | kil | meg | peta | raw | tera | yotta | zetta)

Description

You can use the traffic component to display traffic statistics, including for client, server, Packet Velocity ASIC (PVA), miscellaneous, and authorization traffic. You can also reset the traffic statistics to zero at any time.

Options

For information about the options that you can use with the show command, see show, on page 3-39.

For information about the reset-stats command, see reset-stats, on page 3-31.

See also

reset-stats, show, tmm-info, tmm-traffic, tmsh
UCS

Loads or saves a .ucs file.

Module

sys

Syntax

Configure the ucs component within the sys module using the following syntax.

Modify

save ucs [file name]
  options:
  no-private-key
  passphrase
load ucs [file name]
  options:
  no-license
  no-platform-check
  passphrase
delete ucs [file name]

Display

show ucs [file name]

Description

You can use the ucs component to save the running configuration of the system into a UCS file. Additionally, you can modify the running configuration of the system by loading an existing UCS file.

When you save a UCS file, the file is saved to the default directory, /var/local/ucs.

When you load a UCS file in shell mode, the system searches for the file using the relative path to the default directory (/var/local/ucs). When you load a UCS file in bash mode, the system searches the current directory first. If the file is not found in the current directory, the default directory is then searched.
Examples

Saves the running configuration of the system into the file `myucs.ucs`:
```
save ucs myucs
```

Modifies the running configuration of the system by loading the configuration contained in the `myucs.ucs` file:
```
load ucs myucs
```

Delete `myucs.ucs` in the default directory, `/var/local/ucs/`:
```
delete ucs myucs
```

Displays existing UCS files in the default directory, `/var/local/ucs/`:
```
list ucs
```

Options

You can use the following options with the `ucs` component.

- **no-private-key**
  Indicates that the UCS file can be saved without private key information.

- **passphrase**
  Specifies the passphrase that is necessary to load the specified UCS file.

- **no-license**
  Performs a full restore of the UCS file and all the files it contains, with the exception of the license file.

- **no-platform-check**
  Bypasses the platform check and allows a UCS that is created using a different platform to be installed. By default (without this option), a UCS created from a different platform is not allowed to be installed.

See also

```
list, save, show, tmsh
```

version

Displays software version information for the BIG-IP system.

Module

sys

Syntax

Display statistics for the version component within the sys module using the following syntax.

Display

show version
options:
  detail

Description

You can use the version component to display the software version running on the system, including a list of hot fixes that you have applied to the system.

Examples

Displays software version information:

show version

Displays more extensive software version information about the system, including the operating system kernel information and details about each hot fix that you have applied to the system:

show version detail

Options

For information about the options that you can use with the show command, see show, on page 3-39.

See also

show, tmsh
sys application Module Components

- Introducing the sys application module
- Alphabetical list of components
Introducing the sys application module

You can use the tmsh components that reside within the sys application module to manage application templates and services. For more information about the tmsh hierarchical structure, see Chapter 2, Understanding and Using the Traffic Management Shell.

Alphabetical list of components

The remainder of this chapter lists the tmsh components that are available in the sys application module.
**apl-script**

Provides scripts that can be included by an application template.

**Module**

sys application

**Syntax**

Configure the **apl-script** component within the **sys application** module using the syntax in the following sections.

**Edit**

```
create apl-script [name]
modify apl-script [name]
edit apl-script [ [ [name] | [glob] | [regex] ] ... ]
options:
   all-properties
```

**Display**

```
list apl-script
list apl-script [ [ [name] | [glob] | [regex] ] ... ]
```

**Delete**

```
delete apl-script [name]
```

**Description**

An APL script contains APL that can be directly included in application templates.

APL scripts provide a convenient way to build libraries of common presentation elements.

**Examples**

The following is a fairly simple example of an APL script and a template that makes use of the APL script. The APL script defines a user type that can then be used multiple times in different templates.

```
sys application apl-script com.f5.apl.example {
   define string port validator "PortNumber"
```
Options

You can use these options with the `apl-script` component:

- **description**
  User-defined description.

- **glob**
  Displays the items that match the `glob` expression. See `help glob` for a description of `glob` expression syntax.

- **name**
  Specifies a unique name for the component. This option is required for the commands `create` and `modify`.

- **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. See `help regex` for a description of regular expression syntax.

- **script**
  Contains the APL text that can be imported into application templates.

See also

`delete`, `show`, `list`, `tmsh`, `sys provision`, `sys disk logical-disk`
custom-stat

Provides derived statistics for iStats.

Module

sys application

Syntax

Configure the custom-stat component within the sys application module using the syntax in the following sections.

Edit

create custom-stat [key]
modify custom-stat [key]
options:
  keyspace [string]
  formula [string]
  measure [string]
edit custom-stat [ [ [key] | [glob] | [regex] ] ... ]
options:
  all-properties

Display

list custom-stat
list custom-stat [ [ [key] | [glob] | [regex] ] ... ]

Delete

delete custom-stat [key]

Description

Statistics are derived for objects in the given keyspace based on the given formula, producing the given measure.
Examples

Creates a custom iStat:

```bash
create sys application custom-stat myKey
  keyspace sys.application.service
  measure conns_per_min
  formula "rate counter conns 60"
```

Options

You can use these options with the `custom-stat` command:

- **formula**
  Specifies the first token in the formula indicates the computation to be made. Currently only rates are supported.
  ```bash
  rate <source_measure_type> <source_measure_name>
  <rate_window_in_seconds>
  ```
  Rate computes the rate of change of the source measure over the last `rate_window_in_seconds` seconds. This is applicable only to numeric measures. The derived measure is of type `gauge`.

- **keyspace**
  Specifies that a derived iStat will be computed for all objects in the given keyspace for which the formula is computable (the source measure of the correct type exists).

- **measure**
  Specifies the name of the derived measure to be created. The type of the derived measure is dependent on the formula.

See also

create, modify, sys application app-instance, tmsh
service

Configures traffic management application services.

Module

sys application

Syntax

Modify the service component within the sys application module using the syntax shown in the following sections.

Create/Modify

create service [name]
modify service [name]

options:
  description [string]
  device group [string]
  execute-action [name]
  lists [add | delete | modify | replace-all-with] {
    [name] {
      options:
      value { [string]... }
      value none
    }
  }
lists none
  strict-updates [disabled | enabled]
  tables [add | delete | modify | replace-all-with] {
    [name] {
      options:
      column-names { [name] ... }
      rows { { row { [value] ... } row { [value] ... } ... } }
      rows none
    }
  }
tables none
  template [name]
  traffic group
  variables [add | delete | modify | replace-all-with] {
    [name] {
      options:
value [string]
}
}
variables none
metadata [add | delete | modify] {
    [metadata_name ...] {
        value [ 'value content' ]
        persist [ true | false ]
    }
}
edit service [ [ [name] | [glob] | [regex] ] ... ]
options:
    all-properties
    non-default-properties

Display

list service
list service [ [ [name] | [glob] | [regex] ] ... ]
show running-config service
show running-config service [ [ [name] | [glob] | [regex] ] ... ]
options:
    all-properties
    non-default-properties
    one-line
    partition

Delete

delete service [name]

Options

You can use these options with the service component:

- **description**
  User-defined description.

- **device-group**
  Specifies the name of the device group to which the application service is assigned. If this property is modified with the default keyword, the value of the parent folder or partition will be used, and the inherited-devicegroup property will be set to true.

- **execute-action**
  Runs the specified template action associated with the service.

- **glob**
  Displays the items that match the glob expression. See help glob for a description of glob expression syntax.
◆ lists
Provides the set of list variables and values that are passed to template scripts.

◆ metadata
Associates user defined data, each of which has name and value pair and persistence. The default value is persist, which means the data will be saved into the config file.

◆ regex
Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. See help regex for a description of regular expression syntax.

◆ strict-updates
Specifies whether configuration objects contained in the application service can be directly modified outside the context of the system's application service management interfaces.

◆ tables
Provides the set of table variables and values that are passed to template scripts.

◆ template
Specifies the template that defines the configuration for the application service. This can be changed after the service has been created to move the service to a new template.

◆ template-modified
Indicates that the application template used to deploy the service has been modified. The application service should be updated to make use of the latest changes.

◆ template-prerequisite-errors
Indicates any missing prerequisites associated with the template that defines this application.

◆ variables
The set of atomic variables and values that are passed to template scripts.

See also

create, delete, edit, glob, list, modify, regex, tmsh
**template**

Enables the creation of user-defined templates.

**Module**

`sys application`

**Syntax**

Configure the `template` component within the `sys application` module using the syntax in the following sections.

**Create/Edit/Modify**

- `create template [name]`
- `modify template [name]`

  options:
  - `actions [add | delete | modify | replace-all-with]`
    - `definition`
      - `options`:
        - `html-help [string]`
        - `implementation { [string] }`
        - `presentation { [string] }`
        - `role-acl [add | delete | modify | replace-all-with] {
          - `[role]`
        }`
        - `role-acl none`
        - `run-as [string]`
  - `description [string]`
  - `type [sync-failover | sync-only]`

**Display**

- `edit template [name]`

**Delete**

- `delete template [name]`
Save/Load

```
save template [name] file [filename]
load template [filename]
```

Description

Application templates allow a user to define a custom interface for easily creating complex configurations. The user can create multiple templates for various types of configurations. Once built, the user can use a template to create an application, which is a specific set of configuration objects (such as Virtual IP addresses, pools, and so forth), that work together to perform some task.

The template is composed of two primary parts, the presentation and the implementation.

The presentation section describes a form (a set of questions and user interface elements) that the user must fill out in order to create an application.

The implementation section describes how the values collected from the user (the form variables) are used to generate the actual configuration objects which are part of the application.

The presentation section of the template is written in a simple language called Application Template Language or ATL. The implementation section of the template is written in TCL and provides access to `tmsh` scripting commands.

Application lifecycle

Before describing in detail how a template is written, it is important to understand how the resulting template will be used. Since templates are used to create and edit applications, we examine the application lifecycle.

Application creation

The user selects which template to use for his application. The system presents an empty form, based on the template's presentation script that the user fills out and submits. The system collects and stores the form variables in a newly created application object. Configuration objects are generated based on the form variables by the template's implementation script.

Application editing

The user selects an existing application that he would like to change. The system reloads the form associated with the template that was used to create the application and refills all form variables using the previous user input, which is gathered from the application object. The user edits the form and submits it. The template's implementation script is run again to compute a
new set of configuration objects for the application. The system alters the current configuration objects associated with the application to match the newly computed set of configuration objects, including creating, modifying, and deleting objects as needed.

Application deletion

The user selects an application to delete. All configuration objects associated with the application are removed.

Application Template Language

The application template language describes the user interface presented to a user making a new application, or editing an existing application. It describes what questions to ask, how the questions are presented (for example, a free form field or a list of options), and the names of the variables used to store the values the user inputs.

It consists of a set of primitive form elements (string, number, choice, object), a set of grouping and organization constructs (section, list), methods for hiding or displaying portions of the form based on the values of other portions (optional), and a method to associate human-readable text with various form elements (text).

Primitive Elements

Primitive elements represent the actual user interface components. Each primitive element type is displayed as part of the form, and is associated with a form variable. The following lists the basic primitive types:

- **choice**
  A list of options from which the user can select (a drop-down menu).

  ```
  choice <var-name> [default "<def value>"] [display "<def value>"] {"<choice1>", "<choice2>", ...}
  ```

- **editchoice**
  Multiple choices are available that the user can select, or a new value can be entered if the choices are not acceptable.

  ```
  choice <var-name> [default "<def value>"] [display "<def value>"] {"<choice1>", "<choice2>", ...}
  ```

- **multichoice**
  Similar to a basic choice element except that multiple items can be selected from the available choices.

  ```
  choice <var-name> [default "<def value>"] [display "<def value>"] {"<choice1>", "<choice2>", ...}
  ```

- **password**
  Similar to a string element except the contents can be obscured to prevent others from seeing the value.

  ```
  password <var-name> [default "<def value>"] [display "<def value>"] [required]
  ```
◆ **string**
A basic text box into which the user can enter an arbitrary string.

```
string <var-name> [default "<def value>"] [display "<def value>"] [required] [validator "<validator name>"]
```

Each primitive element is associated with a variable name, which defines where the value collected by the form is stored. In addition, primitive elements can have additional parameters such as a default value, or a validation method, which provides for additional requirements (for example, the string must be an IP address).

The following defines the format for the string primitive values, using normal BNF syntax:

◆ **default**
A sensible default value to which the string is initialized when a new application is created.

◆ **display**
Directs the renderer how to display the element. This can be **small**, medium, large, xlarge, or xxlarge.

◆ **required**
If present, a valid value must be entered before the application can be created

◆ **validator**
The name of a well known validation method.

### Section

The section construct is used to group form variables (primitives) into logical sections for display.

Each section is named, and header text can be defined for a section using the text construct.

Every variable must be inside a section. Sections can be nested, but currently the web-based display of forms limits the section nesting to 2 levels. The format for a section is:

```
section <section-name> { <contents...> }
```

For example, to represent the data associated with a virtual IP:

```
section vip
{
  string addr validator ip
  number port default 80
}
```
Table

The table construct is similar to section, except that it represents a grouping of elements that can be repeated zero or more times. The syntax for table and section are identical.

```plaintext
table <list-name> { <contents...> }
```

For example, to collect a list of nodes from a user to populate a pool, you can add any number of nodes, each of which has a address and port:

```plaintext
section pool
{
    table members
    {
        string address
        string port default "80" display "small"
    }
}
```

The table above is displayed using a JavaScript™ editing widget that enables you to add and remove pool members. Each member contains two form variables: `addr` and `port`.

Optional

The optional construct allows the form elements to be hidden or shown based on the state of other form elements. The syntax of the optional construct is:

```plaintext
optional (<expr>) { <contents...> }
```

The expression in the optional construct is evaluated during the display of the form. The content section is displayed or hidden, based on its value.

To dynamically hide parts of the presentation based on the answer to an earlier question, use the variable name in the expression:

```plaintext
section chooseopts {
    choice show_section_1 {"yes", "no"}
}
section section1 {
    optional (chooseopts.show_section_1 == "yes")
    {
        string str
    }
}
```
Once the user finishes editing an application, the form variables are saved, and the implementation section of the associated template is run. The implementation section is an ordinary TCL script and can use the standard set of tmsh scripting extensions. In addition, there are a few template-specific additions.

First, access to the form variable is done using the following syntax, where \texttt{<section>} is the name of the section to which the variable belongs, and \texttt{<name>} is the name of the form variable:

\begin{verbatim}
$::<section>__<name>
\end{verbatim}

If the variable is in a nested section, the additional sections are also placed before the variable in question, with double underscores between them.

Next, a table can be iterated over, and for each list element, the components of the list can be gathered using the \texttt{tmsh::get_field_value} command. For example, for the pool member example described in the section regarding the list, you can use the following syntax:

\begin{verbatim}
foreach member $::poolmembers {
    set the_addr [tmsh::get_field_value $member addr]
    set the_port [tmsh::get_field_value $member port]
    # Do something with the_addr and the_port
}
\end{verbatim}

Specific details on the application and application templates are provided to the implementation section using built-in variables. Following are the variables available for use.

\begin{itemize}
    \item \texttt{tmsh::app_name}
        Stores the user-provided application name string.
    \item \texttt{tmsh::app_name_path}
        Stores the path name of the application in the configuration database.
    \item \texttt{tmsh::app_template_name}
        Stores the user-provided application template name including the path in the configuration database.
    \item \texttt{tmsh::app_template_action}
        Stores the application template action name.
\end{itemize}
Examples

The following template example shows both the presentation and implementation sections. (It lacks some features, such as use of optional, defaults, validators, etc.)

```plaintext
presentation {
    section basic {
        choice ssl_enabled { "true", "false" }
        string addr
        string more_stuff
        table servers {
            string addr
            string port
            string ratio
        }
    }
    text {
        basic "Some example questions"
        basic.ssl_enabled "Should SSL be enabled?"
        basic.addr "What address should we use for the VIP?"
        basic.servers.addr "Address"
        basic.servers.port "Port"
    }
}

implementation {
    if ( $::basic__ssl_enabled ) {
        set profile_name [format "%s_%s%ssl" $tmsh::app_name clientssl] tmsh::create ltm profile client-ssl $profile_name append profile_name = http
        set destination "$::basic__addr:https"
        set monitor https
    } else {
        set profile_name http
        set destination "$::basic__addr:http"
        set monitor http
    }

    set pool_name [format "%s_%s%pool" $tmsh::app_name pool]
```
set members {
    foreach server $::basic__servers {
        append members [tmsh::get_field_value $server addr] 
        append members ":" 
        append members [tmsh::get_field_value $server port] 
        append members " { ratio " 
        append members [tmsh::get_field_value $server ratio] 
        append members "}" 
        append members " = 
    }
    append members }
}

tmsh::create ltm pool $pool_name \
    members replace-all-with $members \
    monitor $monitor

set vs_name [format "%s_%s" $tmsh::app_name virtual]
tmsh::create ltm virtual $vs_name \
    destination $destination \
    profiles replace-all-with "{ $profile_name }" \
    snat automap \
    pool $pool_name \
    http-class none

**Options**

You can use these options with the **template** component:

- **actions**
  Adds, deletes, or replaces a set of template actions. You can configure the following options for an action:
  - **html-help**
    The help for the application template action formatted as HTML.
  - **implementation**
    The script that is executed to create the configuration objects associated with the application.
  - **name**
    The name of the application template action.
  - **presentation**
    Specifies what questions must be answered to create an application from the template.
  - **role-acl**
    List of roles that are allowed to execute the action.
• **run-as**
The user account that will be used to run the implementation script. If no account is specified, the script is run as the calling user.

• **description**
User-defined description.

• **metadata**
Associates user defined data, each of which has name and value pair and persistence. The default value is `persistent`, which saves the data into the config file.

• **partition**
Displays the administrative partition within which the application template resides.

• **prerequisite-errors**
A message indicating if there are any errors with the prerequisites for the template on the current system. If there are errors no applications can be created from this template. If there are no errors then the template is valid.

• **requires-modules**
Adds, deletes, or replaces the list of modules that are required to be provisioned for this template to work.

• **requires-bigip-version-max**
Specifies the maximum version of software required by this template.

• **requires-bigip-version-min**
Specifies the minimum version of software required by this template.

• **type**
Specifies the types of Device and Traffic groups with which the applications created from this template can be associated.

### Third party Tcl library usage

A selection of third party libraries has been tested to work within the CLI script environment, including MD5, BASE64, SHA1/SHA256, HTTP, TLS, TCL Perl, LDAP client, and XML parser. The TCL packages can only reside in the `/use/share/tcl8.4` directory.

---

**Important**

*Only these tested packages are supported currently.*

The following example shows how the Tcl package command can make use of the XML parser:

```bash
cli script /Common/use_xml {
  proc script::EStart {tag attlist args} {
    array set attr $attlist
    puts "Element "$tag" started with [array size attr] attributes"
  }
```

Traffic Management Shell (tmsh) Reference Guide
proc script::PCData text {
    incr ::count [string length $text]
}

proc script::run {} {
    namespace eval :: {
        set count 0
    }
    puts "running use_xml...\n"
    set pkg_name xml
    if {{catch (package require $pkg_name 3.2)}} {
        puts "No package found: $pkg_name!\n"
    } else {
        puts "Found package: $pkg_name!\n"
        set parser [xml::parser]
        $parser configure -elementstartcommand script::EStart -characterdatacommand script::PCData
        set fp [open "/shared/test.xml" r]
        set text [read $fp]
        $parser parse $text
        puts "The document contains ::count characters"
        close $fp
    }
}

Here are some additional examples:

cli script /Common/use_sha1 {
    proc script::run {} {
        set pkg_name sha1
        if {{catch (package require $pkg_name)}} {
            puts "No package found: $pkg_name!\n"
        } else {
            puts "Found package: $pkg_name!\n"
            puts "TCL does SHA1 now:"
            puts [sha1::sha1 -hex "TCL does SHA1"]
        }
    }
}

cli script /Common/use_base64 {
    proc script::run {} {
        set pkg_name base64
        if {{catch (package require $pkg_name)}} {
            puts "No package found: $pkg_name!\n"
        } else {
            puts "Found package: $pkg_name!\n"
            puts "TCL does Base64 now:"
            puts [base64::encode -hex "TCL does Base64"]
        }
    }
}
else {
    puts "Found package: $pkg_name!\n"
    set chemical [encoding convertto utf-8 "C\u2088H\u2081\u2080N\u2084O\u2082"]
    set encoded [base64::encode $chemical]
    set caffeine [encoding convertfrom utf-8 [base64::decode $encoded]]
    puts "Caffeine: $caffeine"
}

See also

   edit, list, modify, show, tmsh
sys crypto Module Components

- Introducing the sys crypto module
- Alphabetical list of components
Introducing the sys crypto module

You can use the `tmsh` components that reside within the `sys crypto` module to manage cryptographic objects in the system. For more information about the `tmsh` hierarchical structure, see Chapter 2, *Understanding and Using the Traffic Management Shell*.

Alphabetical list of components

The remainder of this chapter lists the `tmsh` components that are available in the `sys crypto` module.
cert

Manages cryptographic certificates on the BIG-IP® system.

Module

sys crypto

Syntax

Manage cryptographic certs using the syntax in the following section.

Create

create cert [name]
    options:
    city [string]
    common-name [string]
    consumer
    [enterprise-manager | iquery | iquery-big3d | ltm | webserver]
    country [string]
    email-address [string]
    lifetime [days]
    organization [string]
    ou [string]
    state [string]

Install

install cert [name]
    options:
    consumer
    [enterprise-manager | iquery | iquery-big3d | ltm | webserver]
    from-editor
    from-local-file [filename]
    from-url [URL]

Delete

delete cert [name]
Description

You can use the `cert` component to create, install, and delete cryptographic certificates, and bundles.

Examples

Generates a self signed certificate named `my.crt`. A key with the corresponding name `my.key` must be installed on the system in order for this operation to succeed:

```
create cert my common-name "My Company Inc." country "US"
```

Generates a self-signed certificate named `server2.crt`. The consumer attribute, `webserver`, is used to cause the files to be placed directly in the path which can be found by the BIG-IP's httpd. A preexisting `server2.key` must exist in the web server's key path in order for this operation to succeed:

```
create cert server2 common-name "My Company Inc." country "US" consumer webserver
```

Opens an interactive editor session into which can be pasted a certificate for import into the BIG-IP system. A certificate file-object will be created with the name example.crt which contains the contents saved from the editor session:

```
install cert example from-editor
```

Opens an interactive editor session into which can be pasted a certificate for import into the BIG-IP system. A certificate file-object will be created with the name example.crt which contains the contents saved from the editor session:

```
install cert example from-local-file /tmp/example.crt
```

Obtains a certificate from a remote host, based on the URI specified:

```
install cert example from-url http://example.com/example.crt
```

Options

- **city**
  Specifies the X.509 city field to be used in creation of the certificate.

- **common-name**
  Specifies the X.509 common-name to be used in creation of the certificate.

- **consumer**
  Specifies the system component by which a certificate will be consumed. The default behavior is to create file-objects for use by Local Traffic Manager™ components. This is the same as specifying `ltm` for this property. If a component other than `ltm` is specified then files will be installed-created in locations where the specified components can find them. For example, for component `webserver`, certificates will be placed in the webserver’s SSL directories.
◆ country
   Specifies the X.509 country to be used in creation of the certificate. The
country must be a 2 letter country code.

◆ email-address
   Specifies the X.509 email-address to be used in creation of the
certificate.

◆ from-editor
   Specifies that the certificate should be obtained from a text editor
session. This allows certificates to be imported using cut-n-paste from
another location as long as they are in a text representation.

◆ from-local-file
   Specifies a local file path from which a certificate is to be copied.

◆ from-url
   Specifies a URI which is to be used to obtain a certificate for import into
the system. The URL syntax is protocol dependent. You can find a
detailed description in RFC 3986. Supported schemes are HTTP,
HTTPS, FTP, FTPS and FILE.

◆ organizationmod
   Specifies the X.509 organization to be used in creation of the certificate.

◆ ou
   Specifies the X.509 organizational unit to be used in creation of the
certificate.

◆ state
   Specifies the X.509 state or province of the certificate.

See also

create, install, delete, tmsh
check-cert

Examines certificates and displays or logs any that have expired on the BIG-IP system.

Module

sys crypto

Syntax

Run a check on the expiration date of LTM™ certificates, in the sys crypto module by using the syntax below.

Run

```
run check-cert [certificate-file-name]

options:
  log [enabled | disabled]
  stdout [enabled | disabled]
  verbose [enabled | disabled]
```

Description

You can use the check-cert command to check the expiration date of certificate(s) and print the results to the screen and/or log them to /var/log/ltm.

Examples

Checks all certificate file-objects known by MCPD, and displays information about any certificates which have expired or which are close to expiration. By default this information is printed to the screen and logged to /var/log/ltm:

```
run check-cert
```

Runs the check on the specific certificate default.crt:

```
run check-cert default.crt
```

Displays expiration information about all certificates, not just those that have expired or have impending expirations:

```
run check-cert verbose
```
Prints the results to screen but does not log them:

```bash
run check-cert log disabled
```

Logs the results to `/var/log/ltm`, but does not print them to the screen:

```bash
run check-cert stdout disabled
```

### Options

- **log**
  Specifies whether results should be logged or not. By default they will be logged.

- **stdout**
  Specifies whether results should be printed to STDOUT or not. By default they will be printed.

- **verbose**
  Specifies whether verbose output should be emitted or not, such as information about all certificates being checked rather than just those which return unfavorable results. By default verbose output is disabled.

### See also

```bash
run, tmsh
```
crl

Manages certificate revocation lists on the BIG-IP system.

Module

sys crypto

Syntax

Manage crls using the syntax in the following section.

Install

install crl [name]
  options:
    ca-file [filename]
    consumer
      [enterprise-manager | iquery | iquery-big3d | ltm | webserver]
    from-editor
    from-local-file [filename]
    from-url [URL]

Delete

delete crl [name]

Description

You can use the crl component to install, and delete certificate revocation lists. The file-objects created by these operations can be used in other BIG-IP configuration blocks such as SSL profiles.

Examples

Opens an interactive editor session into which can be pasted a CRL for import into the BIG-IP system. A CRL file-object will be created with the name example.crl which contains the contents saved from the editor session.

install crl example from-editor

Obtains a CRL from a remote host, based on the URI specified:

install crl example from-local-file /tmp/example.crl

Deletes the certificate revocation list example.crl from the system:

delete crl example
Options

◆ consumer
   Specifies the system component by which the certificate revocation list will be consumed. The default behavior is to create file-objects for use by LTM components. This is the same as specifying ltm for this property. If a component other than ltm is specified then files will be installed or created into locations where the specified components can find them. For example, for component webserver, CRLs will be placed in the webserver’s SSL directories.

◆ from-editor
   Specifies that the CRL should be obtained from a text editor session. This allows CRLs to be imported using cut-n-paste from another location, as long as they are in a text representation.

◆ from-local-file
   Specifies a local file path from which the CRL is to be copied.

◆ from-url
   Specifies a URI which is to be used to obtain the CRL for import into the configuration of the system.
   The URL syntax is protocol-dependent. You can find a detailed description in RFC 3986. Supported schemes are HTTP, HTTPS, FTP, FTPS and FILE.

See also

create, install delete, tmsh
key

Manages cryptographic keys and related objects on the BIG-IP system.

Module

sys crypto

Syntax

Manage cryptographic key and related objects of the sys crypto module using the syntax in the following section.

Create

create key [name]

options:
  city [string]
  common-name [string]
  consumer
    [enterprise-manager | iquery | iquery-big3d | ltm | webserver]
  country [string]
  email-address [string]
  key-size [512 | 1024 | 2048 | 4096]
  key-type [dsa-private | dsa-public | rsa-private | rsa-public]
  organization [string]
  ou [string]
  prompt-for-password
  security-type [fips | normal | password]
  state [string]

Install

install key [name]

options:
  consumer
    [enterprise-manager | iquery | iquery-big3d | ltm | webserver]
  from-editor
  from-local-file [filename]
  from-url [URL]

Delete

delete key [name]
Chapter 41

Description

You can use the key component to create, install, and delete cryptographic keys, and associated cryptographic objects. The file-objects created by these operations can be used in other BIG-IP configuration blocks such as ssl profiles.

Examples

Generates a 2048-bit (default-sized) RSA key file object:

```
create key mykey
```

Generates a 2048-bit (default-sized) RSA key file object and a self-signed certificate named my.key and my.crt respectively. Following a certificate signing request will be printed to the console for use in obtaining a signed certificate from a certificate authority if desired:

```
create key my gen-cert gen-csr common-name "My Company Inc." country "US"
```

Similar to above, but also prompts for a password to be used as a challenge password in the certificate authority signing procedure:

```
create key gen-cert gen-csr my prompt-for-password common-name "My Company Inc." country "US"
```

Generates a key and self signed certificate with file names server2.key and server2.crt. The consumer attribute, webserver, is used to cause these files to be placed directly in the paths which can be found by the BIG-IP system's httpd:

```
create key server2 gen-cert gen-csr common-name "My Company Inc." country "US" consumer webserver
```

Opens an interactive editor session into which can be pasted a key for import into the BIG-IP system. A key file-object will be created with the name example.key which contains the contents saved from the editor session:

```
install key example from-editor
```

Obtains a key from the file located at /tap/example.key:

```
install key example from-local-file /tmp/example.key
```

Obtains a key from a remote host, based on the URI specified:

```
install key example from-url http://example.com/my.key
```

Deletes the key example.key from the system, as well as any existing associated certificate (example.crt) and certificate signing request:

```
delete key example
```

Options

- **city**
  Specifies the X.509 city field to be used in creation of the certificate associated with the given key.
- **common-name**
  Specifies the X.509 common-name to be used in creation of the certificate associated with the given key.

- **consumer**
  Specifies the system component by which a key and/or associated cryptographic file will be consumed. The default behavior is to create file-objects for use by LTM components. This is the same as specifying `ltm` for this property. If a component other than `ltm` is specified, then files will be installed/created into locations where the specified components can find them. For example, for component `webserver`, keys and certs will be placed in the webserver’s SSL directories.

- **country**
  Specifies the X.509 country to be used in creation of the certificate associated with the given key. The country must be a 2 letter country code.

- **email-address**
  Specifies the X.509 email address to be used in creation of the certificate associated with the given key.

- **from-editor**
  Specifies that the key should be obtained from a text editor session. This allows keys to be imported using cut-n-paste from another location as long as they are in a text representation.

- **from-local-file**
  Specifies a local file path from which a key is to be copied.

- **from-url**
  Specifies a URI which is to be used to obtain a key for import into the configuration of the system.

  The URL syntax is protocol dependent. You can find a detailed description in RFC 3986. Supported schemes are **HTTP, HTTPS, FTP, FTPS** and **FILE**.

- **gen-certificate**
  Specifies that in addition to generating a key, a self-signed certificate will also be created. If this option is specified then X.509 attributes should also be specified. Minimally, you must also specify a common-name.

- **gen-csr**
  Specifies that a certificate signing request should be generated along with the key. The CSR will be displayed to the terminal for the purposes of use in getting a certificate signed by an outside authority. X.509 attributes must also be specified.

- **key-size**
  Specifies the size, in bits, of the key to be generated.

- **key-type**
  Specifies the type of cryptographic key to be generated.

- **organization**
  Specifies the X.509 organization to be used in creation of the certificate associated with the given key.
◆ **ou**
   Specifies the X.509 organizational unit to be used in creation of the certificate associated with the given key.

◆ **prompt-for-password**
   Specifies that a password should be prompted for and then used as a challenge password in generation of the CSR (Certificate Signing Request).

◆ **security-type**
   Specifies the level of security used in storing the key in question. For example a security-type of FIPS means that the key should be stored on a FIPS card if one is available.

◆ **state**
   Specifies the X.509 state or province of the certificate associated with the given key.

**See also**

edit, install, delete, tmsh
master-key

Displays the configuration of the master key for the BIG-IP system.

Module

sys crypto

Syntax

Display the configuration of the master-key component within the sys module using the syntax in the following section.

Display

show master-key
options:
  field-fmt

Modify

modify master-key
options:
  prompt-for-password

Run

run master-key diagnostic

Description

You can use the master-key command to manipulate the master key for the system and its peer. You can set it to a value of your choosing by using the prompt-for-password option during a modify. Use the diagnostic option of the run command to test the key integrity.

Examples

Displays, in a table, information about the system's master key:
show master-key

Displays, in field format, information about the system's master key:
show master-key field-fmt
Chapter 41

Load the device key. Uses the device key to decrypt the master key file. Bypasses cached keys to test the integrity of the keys. On success, there is no output. Only if there is an error will there be a response:

```
run master-key diagnostic
```

Create a master-key based on a word or phrase of your choosing. You can use this to manually synchronize several devices without having to copy keys between them:

```
modify master-key prompt-for-password
```

**Options**

For information about the options that you can use with the `show` command, see `show`, on page 3-39.

**See also**

```
show, tmsih
```
**pkcs12**

Install pkcs12 keys and certificates on the BIG-IP system.

**Module**

sys crypto

**Syntax**

Install keys and certificates from pkcs12 files using the syntax in the following section.

**Install**

install pkcs12 [name]

options:

- consumer
  - [enterprise-manager | iquery | iquery-big3d | ltm | webserver]
- from-local-file [filename]
- from-url [URL]
- prompt-for-password

**Description**

You can use the **pkcs12** component to install cryptographic keys and certificates from **pkcs12** formatted files. The file objects created by these operations can be used in other BIG-IP configuration blocks such as SSL profiles.

**Examples**

Obtains a pkcs12 from the file located at /tmp/example.p12, and installs the key and certificate from that file as file objects:

```
install pkcs12 example from-local-file /tmp/example.p12
```

Same as above but also prompts for a password which is to be used to decrypt the **pkcs12** file:

```
install pkcs12 example prompt-for-password from-local-file /tmp/example.p12
```

Obtains a pkcs12 file from a remote host, based on the URL specified:

```
install pkcs12 my from-url http://example.com/my.p12
```
Options

- **consumer**
  Specifies the system component by which a key and associated certificate from a PKCS12 file will be consumed. The default behavior is to create file objects for use by LTM components. This is the same as specifying `ltm` for this property. If a component other than `ltm` is specified then files will be installed/created into locations where the specified components can find them. For example, for component `webserver`, keys and certs will be placed in the webserver’s SSL directories.

- **from-local-file**
  Specifies a local file path from which the contents of the PKCS12 are to be read.

- **from-url**
  Specifies a URI which is to be used to obtain a PKCS12 for import into the configuration of the system.
  
  The URL syntax is protocol dependent. You'll find a detailed description in RFC 3986. Supported schemes are `HTTP`, `HTTPS`, `FTP`, `FTPS` and `FILE`.

- **prompt-for-password**
  Specifies that a password should be prompted for and used to decrypt the PKCS12 file.

See also

install, tmsh
sys crypto fips Module Components

- Introducing the sys crypto fips module
- Alphabetical list of components
Introducing the sys crypto fips module

You can use the tmsh components that reside within the sys crypto fips module to manage components of the fips140 subsystem, when applicable. For more information about the tmsh hierarchical structure, see Chapter 2, Understanding and Using the Traffic Management Shell.

Alphabetical list of components

The remainder of this chapter lists the tmsh components that are available in the sys crypto fips module.
by-handle

Manipulates FIPS 140 keys by-handle.

Module

sys crypto fips

Syntax

Manipulate FIPS 140 keys by-handle within the sys crypto fips module using the syntax in the following section.

Delete

delete by-handle [handle]

Description

You can use the by-handle component to manage the FIPS 140 keys by handle.

You can determine the handle of a FIPS 140 key using the following command:

show sys crypto fips

Examples

Deletes a FIPS 140 key given by the handle 101:

delete by-handle 101

Options

For information about the options that you can use with the delete command, see delete, on page 3-8.

See also

show, tmsh, sys crypto fips private-key, sys crypto fips public-key
private-key

Displays information about FIPS private keys.

Module

sys crypto fips

Syntax

Display information about private-key component within the sys crypto fips module using the syntax in the following section.

Display

show private-key [label]
  options:
    field-fmt
    all-properties

Description

You can use the private-key command to view information about private keys contained in the FIPS hardware.

Examples

Displays the list of all private keys stored in the FIPS hardware and their metadata:

show private-key

Displays information specifically about the FIPS private key(s) which match the label example:

show private-key example

Displays, in field format, information about private keys stored in the FIPS hardware:

show private-key field-fmt

Displays all information about the FIPS contained private keys, including: handle, a numerical value used by the FIPS hardware to identify individual keys; modulus-length, the cryptographic modulus length of the key; and modulus, the modulus associated with the key, displayed as a string of hex octets separated by colons:

show private-key all-properties
Options

For information about the options that you can use with the command `show`, see `show`, on page 3-39.

See also

`show`, `tmsh`
public-key

Displays information about FIPS public keys.

Module

sys crypto fips

Syntax

Display information about public-key component within the sys crypto fips module using the syntax in the following section.

Display

```bash
show public-key [label]
options:
    field-fmt
    all-properties
```

Description

You can use the public-key command to view information about public keys contained in the FIPS hardware.

Examples

Displays the list of all public keys stored in the FIPS hardware and their metadata:

```bash
show public-key
```

Displays information specifically about the FIPS public key(s) that match the label example:

```bash
show public-key example
```

Displays, in field format, information about public keys stored in the FIPS hardware:

```bash
show public-key field-fmt
```

Displays all information about the FIPS contained public keys, including: handle, a numerical value used by the FIPS hardware to identify individual keys; modulus-length, the cryptographic modulus length of the key; and modulus, the value of the cryptographic modulus associated with the key, displayed as a string of hex octets separated by colons:

```bash
show public-key all-properties
```
Options

For information about the options that you can use with the command `show`, see `show`, on page 3-39.

See also

create, install delete, tmsh
sys daemon-log-settings Module
Components

- Introducing the sys daemon-log-settings module
- Alphabetical list of components
Introducing the sys daemon-log-settings module

You can use the `tmsh` components that reside within the `sys daemon-log-settings` module to configure the BIG-IP® system settings and display information about the system. For more information about the `tmsh` hierarchical structure, see Chapter 2, *Understanding and Using the Traffic Management Shell*.

Alphabetical list of components

The remainder of this chapter lists the `tmsh` components that are available in the `sys daemon-log-settings` module.
clusterd

Changes the log-level of or displays information about the daemon clusterd.

Module

sys daemon-log-settings

Syntax

Configure the clusterd component within the sys daemon-log-settings module using the following syntax.

Modify

modify clusterd
   options:
        log-level [critical | debug | error | informational | notice | warning]

edit clusterd
   options:
        all-properties
        non-default-properties

Display

list clusterd
   options:
        all-properties
        non-default-properties
        one-line

Description

You can use the clusterd component to change the level of the messages about the clusterd daemon that appear in the system logs. Additionally, you can display information about the daemon.
Examples

Displays information about the `clusterd` daemon:
```
list clusterd
```

Changes the level of the messages about the `clusterd` daemon that display in the system log to `critical`:
```
modify clusterd log-level critical
```

Options

You can use the following option with the `clusterd` component:

- `log-level`
  Specifies the level of log messages for the specified daemon that you want to display in the system log.

See also

`edit`, `list`, `modify`, `tmsh`
csyncd

Changes the log-level of or displays information about the daemon csyncd.

Module

sys daemon-log-settings

Syntax

Configure the csyncd component within the sys daemon-log-settings module using the following syntax.

Modify

modify csyncd
  options:
    log-level [critical | debug | error | informational | notice | warning]
edit csyncd
  options:
    all-properties
    non-default-properties

Display

list csyncd
  options:
    all-properties
    non-default-properties
    one-line

Description

You can use the csyncd component to change the level of the messages about the clusterd daemon that appear in the system logs. Additionally, you can display information about the daemon.
Examples

Displays information about the csyncd daemon:

```
list csyncd
```

Changes the level of the messages about the csyncd daemon that display in the system log to critical:

```
modify csyncd log-level critical
```

Options

You can use the following option with the csyncd component:

- **log-level**
  Specifies the level of log messages for the specified daemon that you want to display in the system log.

See also

```
edit, list, modify, tmsh
```
**lind**

Changes the log-level of or displays information about the daemon **lind**.

**Module**

```text
sys daemon-log-settings
```

**Syntax**

Configure the **lind** component within the **sys daemon-log-settings** module using the following syntax.

**Modify**

```text
modify lind
options:
  log-level [critical | debug | error | informational | notice | warning]
```

```text
edit lind
options:
  all-properties
  non-default-properties
```

**Display**

```text
list lind
options:
  all-properties
  non-default-properties
  one-line
```

**Description**

You can use the **lind** component to change the level of the messages about the **lind** daemon that appear in the system logs. Additionally, you can display information about the daemon.
Examples

Displays information about the **lind** daemon:

`list lind`

Changes the level of the messages about the **lind** daemon that display in the system log to **critical**:

`modify lind log-level critical`

Options

You can use the following option with the **lind** component:

- **log-level**
  
  Specifies the level of log messages for the specified daemon that you want to display in the system log.

See also

`edit, list, modify, tmsh`
**mcpd**

Changes the log-level of or displays information about the daemon **mcpd**.

**Module**

**sys daemon-log-settings**

**Syntax**

Configure the **mcpd** component within the **sys daemon-log-settings** module using the following syntax.

**Modify**

modify mcpd

options:

- audit [all | disable | enable | verbose]
- log-level [alert | critical | debug | emergency | error | informational | notice | panic | warning]

edit mcpd

options:

- all-properties
- non-default-properties

**Display**

list mcpd

options:

- all-properties
- non-default-properties
- one-line

**Description**

You can use the **mcpd** component to change the level of the messages about the **mcpd** daemon that appear in the system logs. Additionally, you can display information about the daemon.
Examples

Displays information about the `mcpd` daemon:

```
list mcpd
```

Changes the level of the messages about the `mcpd` daemon that display in the system log to `critical`:

```
modify mcpd log-level critical
```

Options

You can use the following options with the `mcpd` component:

- **audit**
  Enables or disables auditing for the `mcpd` daemon, and specifies `verbose` or `all` as the auditing level. The default value is `disable`.

- **log-level**
  Specifies the level of log messages for the specified daemon that you want to display in the system log.

See also

```
edit, list, modify, tmsh
```
tmm

Changes the log-level of or displays information about the Traffic Management Microkernel (TMM).

Module

sys daemon-log-settings

Syntax

Configure the tmm component within the sys daemon-log-settings module using the following syntax.

Modify

modify tmm

options:
  arp-log-level [debug | error | informational | notice | warning]
  http-compression-log-level [debug | error | informational | notice | warning]
  http-log-level [debug | error | informational | notice | warning]
  ip-log-level [debug | informational | notice | warning]
  irule-log-level [debug | error | informational | notice | warning]
  layer4-log-level [debug | informational | notice]
  net-log-level [critical | debug | error | informational | notice | warning]
  os-log-level [alert | critical | debug | emergency | error | informational | notice | warning]
  pva-log-level [debug | informational | notice]
  ssl-log-level [alert | critical | debug | emergency | error | informational | notice | warning]

edit tmm

options:
  all-properties
  non-default-properties

Display

list tmm

options:
  all-properties
  non-default-properties
  one-line
Description

You can use the `tmm` component to change the level of the messages about the TMM that appear in the system logs. Additionally, you can display information about the TMM.

Examples

Displays information about the TMM:

```
list tmm
```

Changes the level of the messages about HTTP compression that display in the system log to `warning`:

```
modify tmm http-compression-log-level warning
```

Options

You can use the following options with the `tmm` component:

- **arp-log-level**
  Specifies the lowest level of ARP messages from the `tmm` daemon to include in the system log. The default value is `warning`.

- **http-compression-log-level**
  Specifies the lowest level of HTTP compression messages from the `tmm` daemon to include in the system log. The default value is `error`.

- **http-log-level**
  Specifies the lowest level of HTTP messages from the `tmm` daemon to include in the system log. The default value is `error`.

- **ip-log-level**
  Specifies the lowest level of IP address messages from the `tmm` daemon to include in the system log. The default value is `warning`.

- **irule-log-level**
  Specifies the lowest level of iRule messages from the `tmm` daemon to include in the system log. The default value is `warning`.

- **layer4-log-level**
  Specifies the lowest level of Layer 4 messages from the `tmm` daemon to include in the system log. The default value is `notice`.

- **net-log-level**
  Specifies the lowest level of network messages from the `tmm` daemon to include in the system log. The default value is `warning`.

- **os-log-level**
  Specifies the lowest level of operating system messages from the `tmm` daemon to include in the system log. The default value is `notice`.  

◆ **pva-log-level**
   Specifies the lowest level of PVA messages from the tmm daemon to include in the system log. The default value is **informational**.

◆ **ssl-log-level**
   Specifies the lowest level of SSL messages from the tmm daemon to include in the system log. The default value is **warning**.

See also

edit, list, modify, tmsh
sys disk Module Components

- Introducing the sys disk module
- Alphabetical list of components
Introducing the sys disk module

You can use the tmsh components that reside within the sys disk module to configure the BIG-IP® system settings, and display information about the system. For more information about the tmsh hierarchical structure, see Chapter 2, Understanding and Using the Traffic Management Shell.

Alphabetical list of components

The remainder of this chapter lists the tmsh components that are available in the sys disk module.
application-volume

Configures an application volume instance.

Module

sys disk

Syntax

Configure the application-volume component in the sys disk module using the syntax shown in the following sections.

Display

show application-volume [name]
lst application-volume [name]

Delete

delete application-volume [name]

Description

The application-volume component provides better granularity for managing disks. Physical disks can now be shared by several application-volumes. An application-volume is physically confined to one logical disk. The visibility of the application-volume can be confined to a particular software volume set or it can be global. No application-volume properties are allowed to be modified through tmsh or iControl® interfaces.

Examples

Deletes an application-volume named mysql_md1.3:

delete application-volume mysql_md1.3

Displays the configuration details of the application-volume mysql_md1.3 in a table:

show application-volume mysql_md1.3
Options

You can use these options with the `application-volume` component:

- **logical.disk [name]**
  Specifies the name of the logical disk in which the application-volume will be created.

- **owner [unassigned/datastor/mysql/vcmp]**
  Specifies the owner for which this application-volume is assigned. The default option is `unassigned`, which means the volume is not in use and nobody owns it.

- **preservability [discardable/precious]**
  Specifies whether the application-volume can be discarded by software (for example, during module provisioning). The default option is `discardable`.

- **resizeable [false/true]**
  Specifies whether the application-volume can potentially be resized. The default option is `false`.

- **size [integer]**
  Specifies the size of the application-volume.

- **volume-set-visibility [name]**
  Specifies the name of the volume set to which the application-volume is constrained, if any.

See also

delete, show, list, tmsh, sys provision, sys disk logical-disk
**logical-disk**

Manages logical disks.

**Module**

**sys disk**

**Syntax**

Configure the logical-disk component in the sys disk module using the syntax shown in the following sections.

**Modify**

```
modify logical-disk [name] 
  options: 
    vg-reserved [integer]
    mode [none/mixed/datastor]
```

**Display**

```
list logical-disk [name]
```

**Description**

The logical-disk component provides better granularity for managing disks. A physical disk can now be shared by one or more logical disks. A logical disk is physically confined to one physical disk.

**Examples**

Modifies the logical disk ldisk1 mode property to mixed and the vg-reserved property size to 200 MiB:
```
modify logical-disk ldisk1 mode mixed vg-reserved 200
```

Displays the configuration details of the logical disk ldisk2:
```
list logical-disk ldisk2
```
Options

- **mode [none/mixed/datasor/control]**
  Specifies the current mode of the logical disk. The options are:
  - **control**
    Indicates that the logical disk is part of a RAID array.
  - **datasor**
    Indicates that the entire disk is committed to the datasor module.
  - **mixed**
    Indicates that the disk contains multiple volumes for software and/or multiple volumes for application data.
  - **none**
    Indicates that the disk is not in use. This is the default option.

- **size [integer]**
  Specifies the size (MiB) of the logical-disk.

- **vg-free [integer]**
  Specifies the usable free space (MiB) available in the logical-disk.

- **vg-in-use [integer]**
  Specifies the total logical-disk space (MiB) in use.

- **vg-reserved [integer]**
  Specifies the reserved logical-disk space (MiB). This space is NOT available for provisioning.

See also

modify, list, tmsh, sys provision, sys disk logical-disk
sys file Module Components

- Introducing the sys file module
- Alphabetical list of components
Introducing the sys file module

You can use the `tmsh` components that reside within the `sys file` module to manage file objects on the system. For more information about the `tmsh` hierarchical structure, see Chapter 2, *Understanding and Using the Traffic Management Shell*.

Alphabetical list of components

The remainder of this chapter lists the `tmsh` components that are available in the `sys file` module.
apache-ssl-cert

Manages an Apache SSL certificate file.

Module

sys file

Syntax

Configure the apache-ssl-cert component within the sys file module using the syntax in the following sections.

Create/Modify

create apache-ssl-cert [name]
modify apache-ssl-cert [name]
options:
source-path [URL]

Display

list apache-ssl-cert
list apache-ssl-cert [ [name] | [glob] | [regex] ] ...

Delete

delete apache-ssl-cert [name]

Description

You can use the apache-ssl-cert component to create, edit, delete, list or modify an Apache SSL certificate.

Examples

Downloads the certificate from the given URL into file-store, creates an SSL certificate file named new-cert, and saves the given URL in the source-path attribute:
create apache-ssl-cert new-cert source-path http:/cert-server/cert_store/certs/cert1.crt

Specifies the location of the file on the local disk (use this when the file has already been created on the local disk):
create apache-ssl-cert new-cert source-path file:/shared/save/cert1.crt
Supported URL format

Supported schemes are HTTP, HTTPS, FTP, FTPS, and FILE.

Options

You can use the following options with the `apache-ssl-cert` component:

- **bundle-certificate**
  Lists data about all the certificates in the bundle, if the certificate file is a bundle; otherwise, this field will be `none`.

- **certificate-key-size**
  Specifies the number of bits in the key associated with this certificate.

- **checksum**
  Specifies a cryptographic hash or checksum of the file contents for use in verification of file integrity.

- **create-time**
  Specifies the time at which the file-object was created.

- **created-by**
  Specifies the user who originally created the file-object.

- **expiration-date**
  Specifies the date at which this certificate expires. Stored as a POSIX time.

- **expiration-string**
  Specifies a string representation of the expiration date of the certificate.

- **fingerprint**
  Specifies the cryptographic fingerprint of the certificate.

- **is-bundle**
  Specifies whether the certificate file is a bundle (that is, whether it contains more than one certificate).

- **issuer**
  Specifies X509 information of the certificate's issuer. If the cert is a bundle, this displays the issuer information for the primary (first) cert in the bundle.

- **key-type**
  Specifies the type of cryptographic key associated with this certificate.

- **last-update-time**
  Specifies the last time at which the file-object was updated/modified.

- **mode**
  Specifies the UNIX file permissions mode for the file associated with this file-object as a numerical value.

- **revision**
  Identifies the latest revision of the file. The revision starts with 1, and increments on each update.

- **serial-number**
  Specifies the certificate's serial number.
◆ size
  Specifies the size (in bytes) of the file associated with this file object.

◆ source-path [URL]
  This attribute takes a URL, for example:
  
  source-path http://cert-server/cert_store/CRLs/backup_10.crl
  source-path https://cert-server/cert_store/CRLs/jan_2010.crl
  source-path ftp://username:password@server/cert_store/CRLs/latest.crl

◆ subject
  Specifies X509 information of the certificate's subject. If the cert is a
  bundle, then this displays the subject information for the primary (first)
  cert in the bundle.

◆ subject-alternative-name
  Specifies a standard X.509 extension dating back as far as 1999 in RFC
  2459.

◆ updated-by
  Specifies the user who last updated the file-object.

◆ version
  Specifies the X509 version of the certificate.

See also

create, delete, edit, glob, list, ltm profile clientssl, ltm profile serverssl,
modify, regex, tmsh
data-group

Manages an external data group file.

Module

sys file

Syntax

Configure the data-group component within the sys file module using the syntax shown in the following sections.

Modify

create data-group [name]
modify data-group [name]
   options:
      data-group-description [string]
      data-group-name [name]
      separator [string]
      source-path [URL]
      type [integer | ip | string ]
edit data-group [ [ [name] | [glob] | [regex] ] ... ]

Display

list data-group
list data-group [ [ [name] | [glob] | [regex] ] ... ]

Delete

delete data-group [name]

Description

You can use the data-group component to create, edit, delete, list or modify an external data group file.
Examples

Downloads the data-group file from the given URL into file-store, creates an external-data-group file named `new-dg`, and saves the given URL in the `source-path` attribute:

```plaintext
create data-group new-dg source-path http://file-server/data-groups/acl.class type string
```

Downloads the data-group file from the given URL into file-store, creates an external-data-group file named `new-dg`, saves the given URL in the `source-path` attribute, and creates an `external` data group within the `ltm data-group` module named `dg` with the given description:

```plaintext
create data-group new-dg source-path http://file-server/data-groups/acl.class type string
data-group-name dg data-group-description "created for rule xyz"
```

Specifies the location of the file on the local disk (use this when the file has already been created on the local disk):

```plaintext
create data-group new-dg source-path file:/shared/save/Test.cls type ip
```

Supported URL format

Supported schemes are HTTP, HTTPS, FTP, FTPS, and FILE.

Options

You can use these options with the `data-group` component:

- **checksum**
  Specifies a cryptographic hash or checksum of the file contents for use in verification of file integrity.

- **created-by**
  Specifies the user who originally created the file-object.

- **create-time**
  Specifies the time at which the file-object was created.

- **data-group-description**
  Specifies the description of the `external` data group that will be created within the `ltm data-group` module and reference the given data group file. This is optional in the `create` command.

- **data-group-name**
  Specifies the name of the `external` data group that will be created within the `ltm data-group` module and reference the given data group file. This is optional in the `create` command.

- **last-update-time**
  Specifies the last time at which the file-object was updated/modified.

- **mode**
  Specifies the UNIX file permissions mode for the file associated with this file-object as a numerical value.
◆ **revision**
   The latest revision of the file. The revision starts with 1, and increments on each update.

◆ **separator**
   Specifies a separator to use when defining the data group. The default value is `:=`.

◆ **size**
   Specifies the size (in bytes) of the file associated with this file object.

◆ **source-path [URL]**
   This attribute takes a URL, for example:
   ```
   source-path http://file-server/data-groups/AUL_1.cls
   source-path https://file-server/data-groups/CNN.x
   source-path ftp://username:password@server/data-groups/latest.class
   ```

◆ **type**
   Specifies the kind of data in the group. This option is required by the command `create`. Possible values for type are:
   - integer
   - ip
   - string

◆ **updated-by**
   Specifies the user who last updated the file-object.

**See also**

create, delete, edit, glob, list, ltm data-group external, modify, regex, tmsh
external-monitor

Manages an external monitor file.

Module

sys file

Syntax

Manage the external-monitor component within the sys file module using the syntax shown in the following sections.

Create/Modify

create external-monitor [name]
modify external-monitor [name]
  options:
    source-path [URL]
edit external-monitor [ [ [name] | [glob] | [regex] ] ... ]

Display

list external-monitor
list external-monitor [ [ [name] | [glob] | [regex] ] ... ]

Delete

delete external-monitor [name]

Description

You can use the external-monitor component to create, edit, delete, list or modify an external-monitor file.
Examples

Downloads the monitor file from the given URL into file-store, creates an external-monitor file named **new-mon**, and saves the given URL in the **source-path** attribute:

```sh
create external-monitor new-mon source-path http://file-server/external-monitors/mon_app1
```

Specifies the location of the file on the local disk (use this when the file has already been created on the local disk):

```sh
create external-monitor new-mon source-path file:/shared/save/Test.mon
```

**Supported URL format**

Supported schemes are **HTTP, HTTPS, FTP, FTPS**, and **FILE**.

**Options**

- **checksum**
  - Specifies a cryptographic hash or checksum of the file contents for use in verification of file integrity.

- **created-by**
  - Specifies the user who originally created the file-object.

- **create-time**
  - Specifies the time at which the file-object was created.

- **last-update-time**
  - Specifies the last time at which the file-object was updated or modified.

- **mode**
  - Specifies the UNIX file permissions mode for the file associated with this file-object as a numerical value.

- **revision**
  - Specifies the latest revision of the file. The revision starts with 1, and increments on each update.

- **size**
  - Specifies the size (in bytes) of the file associated with this file object.

- **source-path [URL]**
  - This attribute takes a URL, for example:
    ```sh
    source-path http://file-server/external-monitors/monitor_service
    source-path https://file-server/external-monitors/custom_mon.1
    source-path ftp://username:password@server/external-monitors/tested.mon
    ```

- **updated-by**
  - Specifies the user who last updated the file-object.
See also

create, delete, edit, glob, list, ltm monitor external, modify, regex, tmsh
ssl-cert

Manages a SSL certificate file.

Module

sys file

Syntax

Configure the ssl-cert component within the sys file module using the syntax in the following sections.

Create/Modify

create ssl-cert [name]
modify ssl-cert [name]
   options:
      source-path [URL]
edit ssl-cert [ [name] | [glob] | [regex] ] ...

Display

list ssl-cert
list ssl-cert [ [name] | [glob] | [regex] ] ...

Delete

delete ssl-cert [name]

Description

You can use the ssl-cert component to create, edit, delete, list, or modify an SSL certificate.

Examples

Downloads the certificate from the given URL into file-store, creates an SSL certificate file named new-cert, and saves the given URL in the source-path attribute:

create ssl-cert new-cert source-path file:/shared/save/cert1.crt

Specifies the location of the file on the local disk (use this when the file has already been created on the local disk):

modify ysshd allow add (192.168.1.245)
Supported URL format

Supported schemes are HTTP, HTTPS, FTP, FTPS, and FILE.

Options

You can use the following options with the ssl-cert component:

- **bundle-certificates**
  Specifies a list of data about all the certificates in the bundle, if the certificate file is a bundle; otherwise, this field will be none.

- **certificate-key-size**
  Specifies the number of bits in the key associated with this certificate.

- **checksum**
  Specifies a cryptographic hash or checksum of the file contents for use in verification of file integrity.

- **create-time**
  Specifies the time at which the file-object was created.

- **created-by**
  Specifies the user who originally created the file-object.

- **expiration-date**
  Specifies the date at which this certificate expires. Stored as a POSIX time.

- **expiration-string**
  Specifies a string representation of the expiration date of the certificate.

- **fingerprint**
  Specifies the cryptographic fingerprint of the certificate.

- **is-bundle**
  Specifies whether the certificate file is a bundle (that is, whether it contains more than one certificate).

- **issuer**
  Specifies X.509 information of the certificate's issuer. If the cert is a bundle, this displays the issuer information for the primary (first) cert in the bundle.

- **key-type**
  Specifies the type of cryptographic key associated with this certificate.

- **last-update-time**
  Specifies the last time at which the file-object was updated/modified.

- **mode**
  Specifies the UNIX file permissions mode for the file associated with this file-object as a numerical value.

- **revision**
  Specifies the latest revision of the file. The revision starts with 1, and increments on each update.

- **serial-number**
  Specifies the certificate’s serial number.
◆ size
   Specifies the size (in bytes) of the file associated with this file object.

◆ source-path> [URL]
   This attribute takes a URL, for example:
   ```
source-path http://cert-server/cert_store/certs/vs_132.crt
source-path https://cert-server/cert_store/certs/vs_132.crt
source-path ftp://username:password@server/cert_store/certs/vs_132.crt
   ```

◆ subject
   Specifies X.509 information of the certificate's subject. If the cert is a
   bundle, then this displays the subject information for the primary (first)
   cert in the bundle.

◆ updated-by
   Specifies the user who last updated the file-object.

◆ version
   Specifies the X.509 version of the certificate.

See also

create, delete, edit, glob, list, ltm profile clientssl, ltm profile serverssl,
modify, regex, tmsh
ssl-crl

Manages a SSL certificate file.

Module

sys file

Syntax

Configure the ssl-crl component within the sys file module using the syntax in the following sections.

Create/Modify

create ssl-crl [name]
modify ssl-crl [name]
    options:
        source-path [URL]
edit ssl-crl [ [ [name] | [glob] | [regex] ] ... ]

Display

list ssl-crl
list ssl-crl [ [ [name] | [glob] | [regex] ] ... ]

Delete

delete ssl-crl [name]

Description

You can use the ssl-crl component to create, edit, delete, list or modify an SSL CRL file.

Examples

Downloads the CRL file from the given URL into file-store, creates an SSL CRL file named new-crl, and saves the given URL in the source-path attribute:

create ssl-crl new-crl source-path http://cert-server/cert_store/CRLs/latest.crl
Specifies the location of the file on the local disk (use this when the file has already been created on the local disk):

```
create ssl-crl new-crl source-path file:/shared/save/copy_10.crl
```

**Supported URL format**

Supported schemes are **HTTP**, **HTTPS**, **FTP**, **FTPS**, and **FILE**.

**Options**

You can use the following options with the `ssl-cert` component:

- **checksum**
  Specifies a cryptographic hash or checksum of the file contents for use in verification of file integrity.

- **created-by**
  Specifies the user who originally created the file-object.

- **create-time**
  Specifies the time at which the file-object was created.

- **last-update-time**
  Specifies the last time at which the file-object was updated/modified.

- **mode**
  Specifies the UNIX file permissions mode for the file associated with this file-object as a numerical value.

- **revision**
  Identifies the latest revision of the file. The revision starts with `1`, and increments on each update.

- **size**
  Specifies the size (in bytes) of the file associated with this file object.

- **source-path [URL]**
  This attribute takes a URL, for example:

  - `source-path http://cert-server/cert_store/CRLs/backup_10.crl`
  - `source-path https://cert-server/cert_store/CRLs/jan_2010.crl`
  - `source-path ftp://username:password@server/cert_store/CRLs/latest.crl`

- **updated-by**
  Specifies the user who last updated the file-object.

**See also**

create, delete, edit, glob, list, ltm profile clientssl, ltm profile serverssl, modify, regex, tmsh
ssl-key

Manages a SSL certificate key file.

Module

sys file

Syntax

Configure the ssl-key component within the sys file module using the syntax in the following sections.

Create/Modify

create ssl-key [name]
modify ssl-key [name]
  options:
    source-path [URL]
    passphrase [passphrase]
edit ssl-key [ [ [name] | [glob] | [regex] ] ... ]

Display

list ssl-key
list ssl-key [ [ [name] | [glob] | [regex] ] ... ]

Delete

delete ssl-key [name]

Description

You can use the ssl-key component to create, edit, delete, list or modify an SSL certificate key file.
Examples

Downloads the certificate-key file from the given URL into file-store, creates an SSL certificate key file named new-key, and saves the given URL in the source-path attribute:

```
create ssl-key new-key source-path http://cert-server/cert_store/certs/cert1.key
```

Specifies the location of the file on the local disk. Use this when the file has already been created on the local disk:

```
create ssl-key new-key source-path file:/shared/save/cert1.key
```

Supported URL format

Supported schemes are HTTP, HTTPS, FTP, FTPS, and FILE.

Options

You can use the following options with the ssl-key component:

- **checksum**
  A cryptographic hash or checksum of the file contents for use in verification of file integrity.

- **create-time**
  Specifies the time at which the file-object was created.

- **created-by**
  Specifies the user who originally created the file-object.

- **key-size**
  The size of the cryptographic key associated with this file object, in bits.

- **key-type**
  Specifies the cryptographic type of the key in question (that is, which algorithm this key is compatible with).

  The options are:
  - **rsa-private**
    The key is an RSA private key.
  - **dsa-private**
    The key is a DSA based private key.

- **last-update-time**
  Specifies the last time at which the file-object was updated/modified.

- **mode**
  Specifies the UNIX file permissions mode for the file associated with this file-object as a numerical value.

- **revision**
  Specifies the latest revision of the file. The revision starts with 1, and increments on each update.

- **security-type**
  Specifies the type of security used to handle or store the key.
The options are:

- **normal**
  The key resides in a standard form on the file-system. This is the default value.

- **fips**
  The key is protected by a FIPS device on the system and is only applicable to devices with FIPS support.

- **password**
  Specifies that the key is protected by a passphrase and stored in encrypted form.

- **size**
  Specifies the size (in bytes) of the file associated with this file object.

- **source-path> [URL]**
  This attribute takes a URL, for example:

  ```plaintext
  source-path http://cert-server/cert_store/certs/vs_132.key
  source-path https://cert-server/cert_store/certs/vs_132.key
  source-path ftp://username:password@server/cert_store/certs/vs_132.key
  ```

- **updated-by**
  Specifies the user who last updated the file-object.

See also

create, delete, edit, glob, list, ltm profile clientssl, ltm profile serverssl, modify, regex, tmsh
sys performance Module Components

- Introducing the sys performance module
- Alphabetical list of components
Introducing the sys performance module

You can use the `tmsh` components that reside within the `sys performance` module to display statistics about the system. For more information about the `tmsh` hierarchical structure, see Chapter 2, *Understanding and Using the Traffic Management Shell*.

Alphabetical list of components

The remainder of this chapter lists the `tmsh` components that are available in the `sys performance` module.
all-stats

Resets or displays all performance statistics.

Module

sys performance

Syntax

Reset or display all performance statistics for the system within the sys performance module using the syntax in the following sections.

Modify

reset-stats all-stats

Display

show all-stats

options:

[default | exa | gig | kil | meg | peta | raw | tera | yotta | zetta]

[detail | historical]

Description

You can use the all-stats component to reset or display all system performance statistics.

◆ Note

tmsh only displays performance statistics when you explicitly request them.

Examples

Displays detailed information about system performance in the system default units:

show all-stats detail

Resets all performance statistics for the system:

reset-stats all-stats
Options

For information about the options that you can use with the commands reset-stats and show, see reset-stats, on page 3-31, and show, on page 3-39.

See also

reset-stats, show, sys performance gtm, sys performance ramcache, sys performance system, sys performance throughput, tmsh
connections

Displays connection performance information.

Module

sys performance

Syntax

Display statistics for the connections component within the sys performance module using the syntax in the following sections.

display

show connections

options:

[default | exa | gig | kil | meg | peta | raw | tera | yotta | zetta]

[detail | historical]

Description

You can use the connections component to display information about system performance, including details about new and active connections and HTTP requests.

You can reset the connection performance statistics using the all-stats component. For more information, see all-stats, on page 46-2.

Examples

Displays detailed information about connection performance in gigabits per second:

show connections gig detail

Displays historical performance information about connections:

show connections historical

Options

For information about the options that you can use with the show command, see show, on page 3-39.
See also

show, sys performance all-stats, sys performance gtm, sys performance ramcache, sys performance system, sys performance throughput, tmsh
gtm

Displays performance information for the Global Traffic Manager™.

Module

sys performance

Syntax

Display statistics for the gtm component within the sys performance module using the syntax in the following sections.

Display

show gtm

options:
[default | exa | gig | kil | meg | peta | raw | tera | yotta | zetta]
[detail | historical]

Description

You can use the gtm component to display information about the Global Traffic Manager, including number of requests, resolutions, persistent connections, and those connections returned to DNS.

You can reset the Global Traffic Manager performance statistics using the all-stats component. For more information, see all-stats, on page 46-2.

Examples

Displays detailed performance information about the Global Traffic Manager in the system default units:

show gtm detail

Displays historical performance information about the Global Traffic Manager:

show gtm historical

Options

For information about the options that you can use with the show command, see show, on page 3-39.
See also

show, sys performance all-stats, sys performance connections, sys performance ramcache, sys performance system, sys performance throughput, tmsh
ramcache

Displays RAM cache performance information.

Module

sys performance

Syntax

Display statistics for the ramcache component within the sys performance module using the syntax in the following sections.

Display

show ramcache

options:
  [default | exa | gig | kil | meg | peta | raw | tera | yotta | zetta]
  historical

Description

You can use the ramcache component to display RAM cache utilization information.

You can reset the RAM cache performance statistics using the all-stats component. For more information, see all-stats, on page 46-2.

Examples

Displays RAM cache performance information in the system default units:

  show ramcache

Displays historical RAM cache performance information:

  show ramcache historical

Options

For information about the options that you can use with the show command, see show, on page 3-39.
See also

show, sys performance all-stats, sys performance connections, sys performance gtm, sys performance system, sys performance throughput, tmsh
sflow-receiver

Manages sFlow receivers configured on the BIG-IP® system.

Module

sys performance

Syntax

Configure the sflow-receiver component within the sys performance module using the syntax in the following sections.

Create/Modify

create sflow-receiver [name]
modify sflow-receiver [name]
   options:
      address [ip address]
      max-datagram-size [integer]
      poll-interval [integer]
      port [ip port]
create zone [name]

Display

list sflow-receiver
list sflow-receiver [ [ [name] | [glob] | [regex] ] ... ]

Delete

delete sflow-receiver [name]

Description

You can use the sflow-receiver component to create, delete, list, or modify an sFlow receiver object on the BIG-IP system.

◆ Note

You can add an sFlow receiver to the BIG-IP system, only if you are assigned either the Resource Administrator or Administrator user role.
**Examples**

Creates an sFlow receiver object named `my_receiver` with an IP address of 10.10.10.10, where the `port`, `max-datagram-size`, and `poll-interval` options are set to default values:

```bash
create sflow-receiver my_receiver address 10.10.10.10
```

Creates an sFlow receiver object named `my_receiver` with an IP address of 10.10.10.10, a port of 1234, and `max-datagram-size` and `poll-interval` options are set to default values:

```bash
create sflow-receiver my_receiver address 10.20.10.20 port 1234
```

**Options**

You can use these options with the `sflow-receiver` component:

- **address**
  Specifies the IP address on which the sFlow receiver listens for UDP datagrams.

- **glob**
  Displays the items that match the `glob` expression. See `help glob` for a description of `glob` expression syntax.

- **max-datagram-size**
  Specifies the maximum size in bytes of the UDP datagram the sFlow receiver accepts.

- **name**
  Specifies a unique name for the component. This option is required for the commands `create`, `delete`, and `modify`.

- **poll-interval**
  Specifies the maximum interval in seconds between polling by the sFlow agent of monitored data sources on the BIG-IP system.

- **port**
  Specifies the port on which the sFlow receiver listens for UDP datagrams. The default value is the standard sFlow port.

- **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. See `help regex` for a description of regular expression syntax.

**See also**

`create`, `delete`, `edit`, `glob`, `list`, `modify`, `regex`, `tmsh`
system

Displays system performance information.

Module

sys performance

Syntax

Display statistics for the system component within the sys performance module using the syntax in the following sections.

Display

show system

options:

[default | exa | gig | kil | meg | peta | raw | tera | yotta | zetta]

[detail | historical]

Description

You can use the system component to display CPU and memory usage information.

You can reset the system performance statistics using the all-stats component. For more information, see all-stats, on page 46-2.

Examples

Displays detailed system performance information in the system default units:

show system detail

Displays historical system performance information:

show system historical

Options

For information about the options that you can use with the show command, see show, on page 3-39.
See also

show, sys performance all-stats, sys performance connections, sys performance gtm, sys performance ramcache, sys performance throughput, tmsh
throughput

Displays performance information about traffic throughput.

Module

sys performance

Syntax

Display statistics for the throughput component within the sys performance module using the syntax in the following sections.

Display

show throughput
  options:
  [default | exa | gig | kil | meg | peta | raw | tera | yotta | zetta]
  [detail | historical]

Description

You can use the throughput component to display information about traffic throughput, including client, server, compression, and SSL transactions.

You can reset the throughput performance statistics using the all-stats component. For more information, see all-stats, on page 46-2.

Examples

Displays detailed throughput performance information in gigabits per second:

show throughput gig detail

Displays historical throughput performance information:

show throughput historical

Options

For information about the options that you can use with the show command, see show, on page 3-39.
See also

show, sys performance all-stats, sys performance connections, sys performance ramcache, sys performance system, sys performance system, tmsh
sys raid Module Components

- Introducing the sys raid module
- Alphabetical list of components
Introducing the sys raid module

You can use the \texttt{tmsh} components that reside within the \texttt{sys raid} module to configure disk arrays and display information about the system arrays, bay, and disks. For more information about the \texttt{tmsh} hierarchical structure, see Chapter 2, \textit{Understanding and Using the Traffic Management Shell}.

Alphabetical list of components

The remainder of this chapter lists the \texttt{tmsh} components that are available in the \texttt{sys raid} module.
array

Configures an array of hard disks on the BIG-IP® system.

Module

sys raid

Syntax

Configure the array component within the sys raid module using the syntax in the following sections.

Modify

modify array [name] [ add | remove ] [hard disk name ]

Display

show array
show array [name]
  options:
    field-fmt

Description

You can use the array component to add a hard disk to or remove a hard disk from an array of disks, or to display information about an array of disks.

Examples

Displays information about all of the arrays that are configured on the system:

show array

Removes hard disk HD2 from array MD1:

modify array MD1 remove HD2
Options

You can use the following options with the array component:

- **hard disk name**
  Specifies the name of the hard disk that you want to add to or remove from the array. This option is required for the modify command.

- **name**
  Specifies the name of the array. This option is required for the modify command.

See also

modify, show, tmsh
bay

Manages a BIG-IP system disk drive bay.

Module

sys raid

Syntax

Manage the bay component within the sys raid module using the syntax in the following sections.

Modify

modify bay [1 | 2]
  options:
    flash-led
    no-flash-led

Display

show bay [1 | 2]
  options:
    field-fmt

Description

You can use the bay component to display information about a system bay, cause the LED on a bay to start flashing, or cause the LED on a bay to stop flashing. The LED is helpful for identifying the location of a specific disk. For more information, see disk, on page 47-6.

Examples

Causes the LED on bay 1 to flash:
modify bay 1 flash-led

Displays information about the system bay:
show bay

Displays information about the system bay in a field format:
show bay field-fmt
Options

You can use the following options with the `bay` component:

- **flash-led**
  Causes the LED on the bay to flash.

- **no-flash-led**
  Causes the LED on the bay to stop flashing.

See also

`show`, `sys raid disk`, `tmsh`
disk

Displays information about the BIG-IP system disks.

Module

sys raid

Syntax

Display information about the disk component within the sys raid module using the syntax in the following sections.

Display

```
show disk [name]
  options:
    field-fmt
```

Description

You can use the disk component to display information about the system disks including name, serial number, and whether the disk is a member of an array of disks. When all-properties option is specified, the media wear-out information of the disk is also shown.

This information includes the wear-out indicator, space available, power-on hours, and estimated remaining life.

Examples

Displays information about all of the system disks:
```
show disk
```

Displays information, in a field format, about disk, HD1:
```
show disk HD1 field-fmt
```

Displays all information (including the media wear-out information) about disk, SSD1:
```
show disk SSD1 all-properties
```
Options

You can use the following options with the `disk` component:

- name
  Specifies the name of the disk for which you want to display information.

See also

show, tmsh
sys software Module Components

• Introducing the sys software module

• Alphabetical list of components
Introducing the sys software module

You can use the `tmsh` components that reside within the `sys software` module to configure the BIG-IP® system settings and display information about the system. For more information about the `tmsh` hierarchical structure, see Chapter 2, *Understanding and Using the Traffic Management Shell*.

Alphabetical list of components

The remainder of this chapter lists the `tmsh` components that are available in the `sys software` module.
hotfix

Manages F5 Networks® software hotfixes.

Module

sys software

Syntax

Install, display information about, or delete a hotfix using the syntax in the following sections.

Install

install hotfix [name] volume [name]
options:
  create-volume
  reboot

Display

list hotfix
list hotfix [ [ name [/slot_id] ] | [glob] | [regex] ] ... ]
options:
  build
  checksum
  id
  one-line
  title
  product
  title
  verified
  version

Delete

delete hotfix [name]
Description

You can use the `hotfix` component to install a hotfix onto a volume, view information about available hotfixes, or delete unwanted hotfixes.

Use the `create-volume` option with the `hotfix` component to create new volumes.

◆ Note

You use the `slot_id` option only for chassis systems and only when displaying the values for the options of a specific image. You do not use the `slot_id` option when installing or deleting an image, because these commands operate on all blades or the entire system.

Examples

Displays information about the specified hotfix, `BIGIP-9.6.1-824.0-HF3.im`:

```
list hotfix Hotfix-BIGIP-9.6.1-824.0-HF3.im
```

Displays information about all the hotfixes on the first slot:

```
list hotfix */1
```

Attempts to install the specified hotfix, `BIGIP-9.6.1-824.0-HF3.im`, onto `HD1.1`:

```
install hotfix Hotfix-BIGIP-9.6.1-824.0-HF3.im HD1.1 reboot
```

◆ Note

If the installation is successful, and you used the `reboot` option, as in this example, the machine reboots into the newly installed hotfix.

Options

You can use these options with the `hotfix` component:

◆ `build`
  Displays the build number of the hotfix.

◆ `checksum`
  Displays the checksum of the hotfix. You can use this option to verify the integrity of the hotfix.

◆ `create-volume`
  Create a new volume using the name specified with the `volume` option. Mirrored volume names must begin with the prefix `MD1`. Mirrored volumes are available only on systems that support RAID, see `sys raid`.

◆ `glob`
  Displays the items that match the `glob` expression. See the `glob` man page for a description of `glob` expression syntax.
◆ **name**
  Specifies the name and sequential ID of the hotfix that you want to install or delete.

◆ **product**
  Displays the F5 Networks product the hotfix contains.

◆ **reboot**
  Specifies that the system reboots immediately after a successful installation.

◆ **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. See the `regex` man page for a description of regular expression syntax.

◆ **slot_id**
  Specifies the number of the slot on a chassis system that contains the hotfix about which you want to display information.

◆ **title**
  Displays a textual description of the hotfix.

◆ **verified**
  When set to `yes`, indicates that the hotfix is authentic.

◆ **version**
  Displays the version number of the product the hotfix contains.

◆ **volume**
  Specifies the name of the volume on which you want to install the hotfix or from which you want to delete the hotfix.

See also

delete, glob, install, list, regex, reboot, sys image, tmsh
image

Manages F5 Networks software images.

Module

sys software

Syntax

Install, display information about, or delete a software image using the syntax in the following sections.

Install

install
  options:
  create-volume
  image [name]
  reboot
  retry
  volume [name]

Display

list image
list image [ [ [ name [/slot_id] ] | [glob] | [regex] ] ... ]
  options:
  build
  build-date
  checksum
  file-size
  last-modified
  one-line
  product
  verified
  version

Delete

delete image [name]
Chapter 48

Description

You can use the `image` component to install images onto a volume, view information about available images, or delete unwanted images.

Using the `create-volume` option, the `image` component is also used to create new volumes.

◆ Note

*You use the `slot_id` option only for chassis systems and only when displaying the values for the options of a specific image. You do not use the `slot_id` option when installing or deleting an image, because these commands operate on all blades or the entire system.*

Examples

Attempts to install the specified image, **BIGIP-10.0.0.5376.0.iso**, onto **HD1.1**. If the installation is successful, the machine reboots into the newly installed image:

```
install image BIGIP-10.0.0.5376.0.iso HD1.1 reboot
```

Displays information about the specified image, **build 5376.0** of **BIG-IP version 10.0.0**:

```
list image BIGIP-10.0.0.5376.0.iso
```

Displays information about all of the images located on the first slot:

```
list image */1
```

Options

You can use these options with the `image` component:

◆ **build**
  Displays the build number of the image.

◆ **build-date**
  Displays the date on which the image was built.

◆ **checksum**
  Displays the checksum of the image. You can use this option to verify the integrity of the image.

◆ **create-volume**
  Creates a new volume using the name specified with the `volume` option. Mirrored volume names must begin with the prefix **MD1**. Mirrored volumes are available only on systems that support RAID, see **sys raid**.

◆ **file-size**
  Displays the size of the image file in megabytes.

◆ **glob**
  Displays the items that match the `glob` expression. See the `glob` man page for a description of `glob` expression syntax.
- **last-modified**
  Displays the date the file was last modified.

- **name**
  Specifies the name of the image that you want to install or delete.

- **product**
  Displays the F5 Networks product the image contains.

- **reboot**
  Specifies that the system reboots immediately after a successful installation.

- **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. See the `regex` man page for a description of regular expression syntax.

- **retry**
  Specifies that the system should continue to try installing the image if there were insufficient resources during the first attempt.

- **verified**
  When set to `yes`, indicates that the hotfix is authentic.

- **version**
  Displays the version number of the product this image contains.

- **volume**
  Specifies the name of the volume on which you want to install the image or from which you want to delete the image.

  **Important:** You cannot install software on the active volume.

### See also

delay, glob, install, list, regex, reboot, sys software hotfix, tmsh
status
Displays the status of a BIG-IP system software installation.

Module
sys software

Syntax
Display information about the status component within the sys software module using the syntax in the following sections.

Display

```plaintext
show status
options:
  field-fmt
```

Description
You can use the status component to display the status of the software installation, including whether the system is active, the name of the product being installed, the software version and build number of the software, and the slot and volume on which the software is installed.

Examples
Displays the status of the software installation in a table:
```plaintext
show status
```

Displays the status of the software installation separately for each volume on the system:
```plaintext
show status field-fmt
```

Options
You can use this option with the status component:

- field-fmt
  Displays the software status for each volume in a field format, rather than in a table.
See also

show, tmsh
volume

Manages software volumes on the BIG-IP system.

Module

sys software

Syntax

Delete, reboot into, or display information about a hard drive volume using the syntax in the following sections.

Reboot

reboot volume [name]

Create/Modify

create volume [name]
reboot volume [name]

Display

list volume
list volume [ [ [name].[slot_id] ] | [glob] | [regex] ] ... ]
show running-config
show running-config [ [ [name].[slot_id] ] | [glob] | [regex] ] ... ]

options:
  active
  active-requested
  all-properties
  basebuild
  build
  edition
  media [media] [size] [default-boot-location]
  one-line
  product
  status
  version

Delete

delete volume [name]
Description

You can use the `volume` component to view information about configured volumes, delete unwanted volumes, and reboot the device to a specific volume.

Volumes are created using the `install` command. See `help sys software image` and the option `create-volume`.

Deleting or rebooting into a volume on a VIPRION® system affects the entire chassis; therefore, you do not need to specify the slot number.

Examples

Displays the details of all the volumes located on the first slot in a chassis:

```
list volume */1
```

Deletes the volume named `HD1.5`:

```
delete volume HD1.5
```

Boots into volume `HD1.1` if that volume is not already active. If the volume has an image actively being installed on it, the reboot occurs when the installation is complete:

```
reboot volume HD1.1
```

Options

You can use these options with the `volume` component:

- **active**
  Specifies whether this volume is being run.

- **active-requested**
  Specifies whether this volume should be active once its status is complete. The system associates this setting with either the active volume or the volume that is going to become active when its status is complete. If `active-requested` is set on a volume that is not presently active, the system reboots into the volume when the volume status is complete. As an example, `install sys software image BIGIP-10.1.0.3341.0.iso volume HD1.2 reboot` will cause `active-requested` to be set on volume HD1.2, and the system will reboot into volume HD1.2 when the installation is complete. This value is read-only.

- **basebuild**
  Displays the build number of either the hotfix presently applied to the system or the original build.

- **build**
  Displays the original build number before any hotfixes.
◆ edition
Displays a textual description of the image. You can use this option to specify the hotfix you want to install.

◆ media
Displays a description of the physical media on which the volume exists. The options are:

• media
  The type of physical device on which the volume exists, for example, hard drive (hd) or compact flash (cf).

• size
  The space on the slot reserved for the volume.

• default-boot-location
  Specifies the volume into which the system boots if the slot resets.

◆ name
Specifies the name of the volume you are configuring. Volume names are in the format HDX.Y, CFX.Y, or MDX.Y, where X is the hard drive index (HDX), compact flash index (CFX), or RAID index (MDX) (on systems that support RAID), and Y is the volume number on that drive.

◆ product
Displays the F5 Networks product that is installed on the volume.

◆ reboot
Reboots the system into the specified volume.

◆ regex
Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. See the regex man page for a description of regular expression syntax.

◆ status
Displays the installation status of the volume. The options are complete or installing.

◆ version
Displays the version number of the software installed on the volume.

See also
delete, glob, install, list, reboot, regex, sys software hotfix, sys software image, tmsh
util Module Components

- Introducing the util module
- Alphabetical list of components
Introducing the util module

You can use the `tmsh` components that reside within the `util` module to run utilities from within the shell. For more information about the `tmsh` hierarchical structure, see Chapter 2, *Understanding and Using the Traffic Management Shell*.

Alphabetical list of components

The remainder of this chapter lists the `tmsh` components that are available in the `util` module.
test-monitor

Runs an external monitor and displays the inputs to and output from the monitor.

Module

util

Syntax

Run the test-monitor utility from within the util module using the following syntax:

```
run util test-monitor <monitor-name> address <ip-address> port <port>
```

Description

The test-monitor utility runs a single instance of a monitor against the specified ip-address:port. The utility output shows the environment, command-line arguments, and resulting messages on stdout and stderr. Internal monitors are not supported.

Examples

Runs a monitor on the IP address 10.10.10.4 and port 80:

```
run util test-monitor monitorA address 10.10.10.4 port 80
```

See also

run, tmsh
tracepath

Runs the `tracepath` utility from within `tmsh`.

Module

`util`

Syntax

Run the `tracepath` utility from within the `util` module using the following syntax:

```
run tracepath [arguments]
```

Read about the arguments that are available for the `tracepath` utility by accessing the help page from within the `util` module using the following syntax:

```
help tracepath
```

Description

**WARNING**

When you are building a batch mode transaction in `tmsh`, if you type the `run` command, the system runs the specified program immediately. It does not add the `run` command to the transaction that you are building.

See also

`bash, cmode, dig, domain-tool, fips-card-sync, fips-util, imish, netstat, help, ping ping6, qkview, run, ssldump, tcpcap, tracepath, tracepath6, traceroute, traceroute6, tmsh, vconsole, zebos`
tracepath6

Runs the **tracepath6** utility from within **tmsh**.

**Module**

**util**

**Syntax**

Run the **tracepath6** utility from within the **util** module using the following syntax:

```
run tracepath6 [arguments]
```

Read about the arguments that are available for the **tracepath6** utility by accessing the help page from within the **util** module using the following syntax:

```
help tracepath6
```

**Description**

**WARNING**

When you are building a batch mode transaction in **tmsh**, if you type the **run** command, the system runs the specified program immediately. It does not add the **run** command to the transaction that you are building.

**See also**

bash, ccmode, dig, domain-tool, fips-card-sync, fips-util, imish, netstat, help, ping, ping6, qkview, run, ssldump, tcpdump, tracepath, traceroute, traceroute6, tmsh, vconsole, zebos
**traceroute**

Runs the `traceroute` utility from within `tmsh`.

**Module**

`util`

**Syntax**

Run the `traceroute` utility from within the `util` module using the following syntax:

```plaintext
run traceroute [arguments]
```

Read about the arguments that are available for the `traceroute` utility by accessing the help page from within the `util` module using the following syntax:

```plaintext
help traceroute
```

**Description**

⚠️ WARNING

When you are building a batch mode transaction in `tmsh`, if you type the `run` command, the system runs the specified program immediately. It does not add the `run` command to the transaction that you are building.

**See also**

bash, ccmode, dig, domain-tool, fips-card-sync, fips-util, imish, netstat, help, ping ping6, qkview, run, ssldump, tcpdump, tracepath, tracepath6, traceroute6, tmsh, vconsole, zebos
traceroute6

Runs the traceroute6 utility from within tmsh.

Module

util

Syntax

Run the traceroute6 utility from within the util module using the following syntax:

run traceroute6 [arguments]

Read about the arguments that are available for the traceroute6 utility by accessing the help page from within the util module using the following syntax:

help traceroute6

Description

◆ WARNING
When you are building a batch mode transaction in tmsh, if you type the run command, the system runs the specified program immediately. It does not add the run command to the transaction that you are building.

See also

bash, cmode, dig, domain-tool, fips-card-sync, fips-util, imish, netstat, help, ping ping6, qkview, run, ssldump, tcpdump, tracepath, tracepath6, traceroute, tmsh, vconsole, zebos
vconsole

Runs the vconsole utility from within tmsh.

Module

util

Syntax

Run the vconsole utility from within the util module using the following syntax:

run vconsole [arguments]

Read about the arguments that are available for the vconsole utility by accessing the help page from within the util module using the following syntax:

help vconsole

Description

⚠️ WARNING

When you are building a batch mode transaction in tmsh, if you type the run command, the system runs the specified program immediately. It does not add the run to the transaction that you are building.

See also

bash, cmode, dig, fips-card-sync, fips-util, imish, help, ping6, qkview, run, ssldump, tcpdump, tracepath, tracepath6, traceroute, traceroute6, tmsh, vconsole, zebos
zebos

Runs the *zebos* utility from within *tmsh*.

Module

*util*

Syntax

Run the *zebos* utility from within the *util* module using the following syntax:

```plaintext
run zebos [arguments]
```

Read about the arguments that are available for the *zebos* utility by accessing the help page from within the *util* module using the following syntax:

```plaintext
help zebos
```

Description

**WARNING**

*WARNING* 
When you are building a batch mode transaction in *tmsh*, if you type the *run* command, the system runs the specified program immediately. It does not add the *run* to the transaction that you are building.

See also

`bash, ccmode, dig, domain-tool, fips-card-sync, fips-util, imish, help, ping, ping6, qkview, run, sldump, tcdump, tracpath, tracpath6, traceroute, traceroute6, tmsh, vconsole`
vcmp Module Components

• Introducing the vcmp module
• Alphabetical list of components
Introducing the vcmp module

You can use the tmsh components that reside within the vcmp module to manage vCMP™ guests and virtual disk images. For more information about the tmsh hierarchical structure, see Chapter 2, Understanding and Using the Traffic Management Shell.

Alphabetical list of components

The remainder of this chapter lists the tmsh components that are available in the vcmp module.
global

Display global vCMP system statistics.

Module

vcmp

Syntax

Configure the global component within the vcmp module using the syntax in the following sections.

Create

copy global

display global

options:
(default | exa | gig | kil | meg | peta | raw | tera | yotta | zetta)

Display

show ucs [file name]

Description

Use the global component within the vcmp module to display high-level vCMP system statistics on a per-slot basis. These are statistics that are not associated with any particular vCMP guest or virtual-disk.

Examples

Display all global vCMP system statistics:

show vcmp global

Options

For information about the options that you can use with the show command, see help show.

See also

tmsh, show, vcmp guest, vcmp vdisk
guest

Configures a cluster of virtual machines (VMs) that run on one or all slots. This cluster is known as a vCMP guest.

Module

vcmp

Syntax

Configure the guest component within the vcmp module using the syntax in the following sections.

Create

create guest [name]
modify guest [name]
options:
  hostname [hostname]
  initial-image [image-filename]
  management-gw [ip-address]
  management-ip [ip-address/netmask|ip-address/prefixlen]
  management-network [bridged|isolated]
  slots [single|all]
  state [configured|provisioned|deployed]
  virtual-disk [filename]
  vlans [add | delete | replace-all-with] {
    [VLAN name] ...
  }

Display

list guest
show guest
options:
  all-properties

Delete

delete guest [name]

Description

Manage guests running on this host.
Examples

Lists the current configuration of all guests:

```
list vcmp guest
```

Displays detailed information regarding the state and progress of all guests:

```
show vcmp guest
```

Displays greater detailed statistics and information of all guests:

```
show vcmp guest all-properties
```

Creates a guest spanning all available slots, with the given management IP and gateway, and with the image file `BIGIP-11.0.0.2400.0.iso`, which is used to initially install TMOS® on the guest's virtual disks. By default, this guest is in the Configured state and has a management network in Bridged mode:

```
create vcmp guest my_guest slots all management-ip 192.168.45.12/24 management-gw 192.168.45.254 initial-image BIGIP-11.0.0.2400.0.iso
```

Moves the guest into the Provisioned state, which causes the hypervisor to allocate hardware resources and create virtual disks for the guest:

```
modify vcmp guest my_vcmp state provisioned
```

Moves the guest into the Deployed state, which causes the hypervisor to start and maintain VMs on each slot for which the guest has resources allocated:

```
modify vcmp guest my_vcmp state deployed
```

Moves the guest back to the Configured state, which causes all of its VMs to shut down and the hardware to be deallocated. (The virtual disks remain on the system, but become unattached to any guest.):

```
modify vcmp guest my_vcmp state configured
```

Modifies the guest to run on a single slot only:

```
modify vcmp guest my_vcmp slots single
```

Options

You can use these options with the `guest` component:

- **hostname**
  Assigns the specified host name to the guest. The host name must be a FQDN. If none is given, the default of `<vcmp_guest_name>.localdomain` is used. If the guest's name contains characters not allowed in a FQDN, then `localhost.localdomain` is used. This is only a suggested value and can be changed on the guest itself. If the guest ever reverts to the default host name, the suggested host name is used instead of the normal system default.
- **initial-image**
  Specifies which TMOS software image to install on newly-created virtual disks for this guest. This image is only used when initially creating the virtual disks. After initial creation, the typical live-install process is used on the guest VMs to manage software upgrades. The image file name must match a verified software image file that exists in the `/shared/images` directory; otherwise, the guest switches to a wait state on any slot on which the image does not exist, until that image is added.

- **management-gw**
  Specifies the IP address of the default gateway for the management network. This IP address is only a suggested value and can be changed on the guest itself. If the guest ever reverts to the default management gateway, the suggested gateway is used instead of the normal system default.

- **management-ip**
  Specifies the management IP address and netmask to assign to the guest. This address floats to the primary slot of the guest. This is only a suggested value and can be changed on the guest itself. If the guest ever reverts to the default management IP address, the suggested IP address is used instead of the normal system default.

- **management-network**
  Specifies the management network mode for this guest. When in Bridged mode, the management interfaces on the guest's VMs are bridged to the physical management interfaces on the host blades. This enables the guest to communicate with networks attached to these physical interfaces, the host itself, and other guests in Bridged mode.

  In Isolated mode, the management interfaces of the guest's VMs are completely disconnected. The only way to manage such a guest is by connecting to the console on each of the guest's VMs by using the `/usr/bin/vconsole` utility or by connecting through a configured self IP on a guest's VLAN. The default value is `bridged`.

- **slots**
  Specifies the number of slots to which this guest should be allocated. When set to `single`, the guest is allocated to the slot with the most available CPU cores not already allocated to other guests. When set to `all`, the guest is allocated to each slot with an available blade.

  Note that this property can be changed while the guest is in any state. While in the Configured state, modifying the `slots` property has no effect, since the guest has not yet been allocated to any slots. While in the Provisioned state, a `single` to `all` modification causes the guest to be allocated to each available slot that it is not already allocated. If this is not possible, an error is given and the guest's allocation is not changed. An `all` to `single` change causes the guest to be de-allocated from all but one slot. The slot to which the guest is allocated is the one with the least number of allocated guests. This same behavior occurs when modifying the property while the guest is in the Deployed state, except that running
VMs are shut down on any slots that the guest is de-allocated from, and new VMs are deployed on any slots to which the guest has been newly allocated.

- **state**
  Guests are put into the Configured state by default. In this state, the configuration for the guest exists on the host, but none of the guest's VMs are running and no hardware resources (for example: CPU cores, memory) are allocated to it. When the guest moves to the Provisioned state, hardware resources are allocated to it, and if not already present, virtual disks are created, and TMOS is installed onto them. In the Deployed state, the `vcmpd` daemon on the host blades use the allocated resources to launch the VMs. Note that moving from the Configured state to the Deployed state implies the actions that occur in the Provisioned state. To shut down a guest's VMs without de-allocating its hardware resources, move the guest from the Deployed state to the Provisioned state. Moving a guest to the Configured state causes its hardware resources to be de-allocated. This does not cause the guest's virtual disks to be deleted. They persist on disk and are reused when the vCMP moves back to the Provisioned/Deployed states.

- **virtual-disk**
  Specifies the file name of the virtual disk to use for this guest's VMs. This is a hint for `vcmpd` when it looks for virtual disk images. If set, the virtual disk name is first verified, if the name ends in the extension `.img`. If not, the extension `.img` is added to the given virtual disk name. Then the modified virtual disk name is verified if the name does not already exist. If the name already exists, an error occurs. If the virtual disk file name ends in `.img`, the name remains unmodified. When a guest moves from the Configured state to the Provisioned state, for each slot that the guest has been allocated to, `vcmpd` first looks for a virtual disk image with the file name from above, in the file `/shared/vmdisks` and then uses it if it exists. If it does not exist, `vcmpd` creates a virtual disk image with the file name. If this property is not set, `vcmpd` creates a new virtual disk file and names it after the guest itself (for example, `my_guest.img`). If a virtual disk with this default name already exists, the system displays an error. This prevents such virtual disks from accidentally being reused.

- **vlans**
  Specifies the list of VLANs configured on the host that should be passed to the guest. These VLANs are automatically configured on the guest on first boot and can be renamed. The tags that the VLANs pass to guests are the only tags that the guest's VMs can use to pass traffic.

See also

create, delete, list, modify, tmsh
vdisk

Manages the vCMP virtual disks available on this hypervisor.

Module

vcmp

Syntax

Configure the vdisk component within the vcmp module using the syntax in the following sections.

Display

list vdisk
  options:
    all-properties
show vdisk

Delete

delete vdisk [name]

Description

The vdisk component is used to list and delete virtual disks that are used by vCMP guests. Virtual disks are automatically created by vcmpd when guests move to the Provisioned state and do not already have virtual disks attached to them. This is the only way that virtual disks are created. Virtual disks that are not attached to any guest can be deleted. Virtual disks not already in use can be explicitly attached to vCMP guests.

Examples

Lists all virtual disks currently available:

list vcmp vdisk

Deletes the virtual disk named my_vdisk. Note that this is only valid if the virtual disk is not currently attached to any vCMP guest:

delete vcmp vdisk my_vdisk
See also

create, delete, list, modify, tmsh
wam Module Components

- Introducing the wam module
- Alphabetical list of components
Introducing the wam module

You can use the tmsh components that reside within the wam module to configure BIG-IP® WebAccelerator™. For more information about the tmsh hierarchical structure, see Chapter 2, Understanding and Using the Traffic Management Shell.

Alphabetical list of components

The remainder of this chapter lists the tmsh components that are available in the wam module.
application

Configures application-wide parameters for WebAccelerator.

Module

wam

Syntax

Configure the application component within the wam module using the syntax shown in the following sections.

Create/Modify

create application [name]
mapping application [name]
options:
  code [number]
  content-expiration-time [date and time]
  description [string]
  metadata-cache-max-size [number]
  hosts [add | delete | modify | replace-all-with] {
    [ [host name] | [glob] ] {
      options:
        code [number]
        subdomain-number-of-http [number]
        subdomain-number-of-https [number]
        subdomain-prefix [string]
    }
  }
  ibr-adaptive-lifetime
  ibr-default-lifetime [number]
  ibr-prefix [string]
  info-header [none | standard | debug]
  policy [name]
  perf-monitor [enabled | disabled]
  perf-monitor-data-retention-period [number]
  send-metadata [never | always | uncompressed]
edit application [ [ [name] | [glob] | [regex] ] ... ]
options:
  all-properties
  non-default-properties
wam Module Components

Traffic Management Shell (tmsh) Reference Guide

reset-stats application

reset-stats application 

list application

show running-config application

options:
  all-properties
  non-default-properties
  partition
  predefined

show application

show application 

options:
  all-properties
  (default | exa | gig | kil | meg | peta | raw | tera | yotta | zetta)
  detail
  field-fmt

Delete

delete application

Note

You must remove all references to an application before you can delete it.

Description

You can use the application component to configure the host map, select policies, and set application-wide parameters that affect WebAccelerator behavior.

Examples

You can use the application component to configure the host map, select policies, and set application-wide parameters that affect WebAccelerator behavior.

create application my_app hosts add { host1.com host2.com } local-policy my_local_policy

Sets the number of subdomain hosts to 3 and the subdomain prefix to abcd for host1.com of WebAccelerator application my_app:

modify application my_app modify hosts { host1.com { subdomain-number-of-http 3 subdomain-prefix abcd } }
Deletes WebAccelerator application **my_app**:

delete application my_app

**Options**

You can use these options with the **application** component:

- **code**
  Specifies a numeric non-zero code of the application or application host, which is used for troubleshooting and performance reporting. Each application or application host must have a unique code. If not supplied by the user, the code is generated by the system. Use the keyword **generate** to specify that the system generate a new unique code.

- **content-expiration-time**
  Specifies the date and time that limits how old cached documents can be to still be served from the cache. All documents older than this date and time are considered expired. For example, the following example expires all cached documents of the application **my_app**:

  ```
  modify application my_app content-expiration-time now
  ```

- **description**
  Describes the object type.

- **hosts**
  Specifies the list of domain names (host names) that might appear in HTTP requests for your web application. These are the same host names that DNS has mapped to the server machine on which your WebAccelerator system is running. To map a group or range of requested host names to a single destination host, you can use an asterisk (*) as a wildcard for the first part of the host name.

- **ibr-adaptive-lifetime**
  Specifies the adaptive lifetime for Intelligent Browser Referencing in seconds. The default value is **864000** (10 days).

- **ibr-default-lifetime**
  Specifies the lifetime for Intelligent Browser Referencing in seconds. The default value is **15724800** (6 months).

- **ibr-prefix**
  Specifies a prefix for the Intelligent Browser Referencing tag. The default value is ";%wa".

- **info-header**
  Enables and controls the appearance of HTTP header **X-WA-Info**: in responses from WebAccelerator. This header can be used for troubleshooting the WebAccelerator system and for tuning policies. The possible values are:

  - **none**
    HTTP header **X-WA-Info**: is not included in responses.

  - **standard**
    HTTP header **X-WA-Info**: is included in responses with standard information, such as S-code, policy, and node codes.
• debug
  HTTP header X-WA-Info: is included in responses with standard information, with some additional values to aid WebAccelerator troubleshooting.

◆ metadata-cache-max-size
  Specifies the maximum size of metadata cache in megabytes. The default size is 25 megabytes.

◆ partition
  Displays the administrative partition within which the application resides.

◆ perf-monitor
  Specifies whether performance monitoring for this application is enabled. Enabling performance monitoring on many applications can affect the overall performance of WebAccelerator. The default value is disabled.

◆ perf-monitor-data-retention-period
  Specifies the time period in days for how long the performance data must be preserved. The default value is 30 days.

◆ policy
  Specifies the acceleration policy to which you want to assign the new web application.

◆ predefined
  Displays whether this application is predefined.

◆ send-metadata
  Specifies when the metadata HTTP header is included in responses. The default value is always. The possible values are:
  • always
    Metadata HTTP header is always included in responses.
  • never
    Metadata HTTP header is not included in responses.
  • uncompressed
    Metadata HTTP header is included only if response is uncompressed.

◆ subdomain-number-of-http
  Specifies the number of HTTP subdomains that you want the WebAccelerator system to generate. The WebAccelerator system uses these additional subdomains only on embedded URLs or links that request images or scripts. The default value is 0.

◆ subdomain-number-of-https
  Specifies the number of HTTPS subdomains that you want the WebAccelerator system to generate. The WebAccelerator system uses these additional subdomains only on embedded URLs or links that request images or scripts. The default value is 0.

◆ subdomain-prefix
  Specifies the prefix that you want the system to assign to the subdomains. The default value is wa.
For example, if the Requested Host is www.siterequest.com, and you select 2 from the HTTP Subdomains box and type wa in the Subdomain Prefix box, the WebAccelerator system changes the domain on qualifying embedded URLs and links to use the following domains:

- wa1.www.siterequest.com
- wa2.www.siterequest.com

*Note:* You must configure DNS with these entries, and they must map to the same IP address as the base origin server (www.siterequest.com in this example).

See also

create, delete, edit, glob, list, modify, regex, reset-stats, show, tmsh
normalization

Configures the URL Normalization settings for WebAccelerator.

Module

wam global-settings

Syntax

Configure the normalization component within the wam global-settings module using the syntax shown in the following sections.

Create/Modify

modify normalization

options:
- add-extension [enabled | disabled]
- auth [enabled | disabled]
- base-path [file path]
- description [string]
- enabled [yes | no]
- groups [add | delete | modify | replace-all-with] {
  [object type group] {
    ...
  }
- normalize-to-browser [enabled | disabled]
- size-threshold [number]
- types [add | delete | modify | replace-all-with] {
  [object type] {
    ...
  }

Display

list normalization
list normalization [option name]
show running-config normalization
show running-config normalization [option name]

options:
- all-properties
- non-default-properties
- one-line
Description

You can use the **normalization** component to configure URL normalization. When the WebAccelerator system receives a response, it analyzes the contents of the response and creates an object ID based on the specific content. To recognize content independent of its URL, the WebAccelerator system inserts the object ID it created into the response that it returns to the client. This process is called URL normalization.

Examples

- Enables the URL normalization feature:
  ```
  modify normalization enabled yes
  ```

- Enables URL normalization for all object types within the group **pages**:
  ```
  modify normalization groups add { pages }
  ```

- Enables URL normalization for the object type **includes.all**:
  ```
  modify global-settings normalization types add { includes.all }
  ```

- Displays the URL normalization settings:
  ```
  list normalization
  ```

Options

You can use these options with the **normalization** component:

- **add-extension**
  Specifies whether the WebAccelerator system should append the URL with a default extension, if the URL does not already contain an extension. When enabled, the WebAccelerator system appends the URL with the default extension for the specific object type. For example, the WebAccelerator system will append document object types with a `.doc` extension. This enables the browser to use the correct application when displaying content for specific object types.

- **auth**
  Specifies whether the WebAccelerator system should require authorization from a client, before providing a requested document. Also, specifies the method on which authorization is based. When enabled, the WebAccelerator system encrypts the object ID and user identifier before using it for the URL redirect, and requires that the user and requested document match, before the WebAccelerator system uses the redirect to retrieve the requested document. To ensure that only authorized clients receive content, we recommend that you enable this feature when you enable the URL Normalization to Browsers feature. The default value is **disabled**. The possible values are:
  - **cookie**
    HTTP header **X-WA-Info**: is not included in responses.
- **disabled**
  HTTP header **X-WA-Info**: is included in responses with standard information, such as S-code, policy, and node codes.

- **url**
  HTTP header **X-WA-Info**: is included in responses with standard information, with some additional values to aid WebAccelerator troubleshooting.

- **base-path**
  Specifies the virtual path on your web site, from which normalized objects appear to originate. The default value is `/pv_obj_cache`. You can change this value for consistency with other URLs on your web site, so that objects appear to come from specific parts of your application. The path must begin with a forward slash (`/`).

- **description**
  Specifies the symmetric deployment description.

- **enabled**
  Enables URL normalization for the configured object types. The default value is `no`.

- **groups**
  Specifies the object type groups to which the WebAccelerator system should apply URL normalization.

- **normalize-to-browser**
  Specifies whether URL normalization to browsers is enabled. If enabled, prompts the WebAccelerator system to enter an object ID in the response header that it returns to the client and store the content in the client browser’s cache for future requests.

- **size-threshold**
  Specifies the minimize size, in kilobytes, required for an object before the WebAccelerator system will apply URL normalization to it. In most cases, the default value of **20KB** is sufficient. For sites with very low bandwidth and low latency links, lowering the value can increase performance. For sites with high bandwidth and high latency links, raising the value can increase performance.

- **types**
  Specifies to which object types the WebAccelerator system should apply URL normalization.

**See also**

`list`, `modify`, `show`, `tmsh`
object-type

Configures object types for WebAccelerator.

Module

wam

Syntax

Configure the object-type component within the wam module using the syntax shown in the following sections.

Create/Modify

create object-type [name]
modify object-type [name]

options:
  code [ [number] | generate]
  compression [disabled | policy-controlled]
  description [string]
  extensions [add | delete | modify | replace-all-with] {
    [document extension]
    ...
  }
  mime-types [add | delete | modify | replace-all-with] {
    [MIME type]
    ...
  }
edit object-type [ [ [name] | [glob] | [regex] ] ... ]

options:
  all-properties
  non-default-properties

Display

list object-type [ [ [name] | [glob] | [regex] ] ... ]
show running-config object-type [ [ [name] | [glob] | [regex] ] ... ]

options:
  all-properties
  non-default-properties
  group
  partition
  predefined
Delete

```
delete object-type [name ...]
```

Description

You can use the `object-type` component to manage recognized types of objects. These object types are used to classify documents processed by WebAccelerator. A document can be classified by its file extension or MIME type.

Examples

Creates a WebAccelerator object type named `documents.abcd` that includes all documents with extensions `.abc` or `.abcd`, and MIME types `text/abcd` or `text/x-abcd`:

```
create object-type documents.abcd extensions add { abc abcd } mime-types add { text/abcd text/x-abcd }
```

Deletes the pool named `documents.abcd`:

```
delete object-type documents.abcd
```

Sets the number of subdomain hosts to 3 and the subdomain prefix to `abcd` for host `host1.com` of WebAccelerator application `my_app`:

```
modify application my_app modify hosts { host1.com { subdomain-number-of-http 3 subdomain-prefix abcd } }
```

Displays properties of the object-type named `documents.abcd`:

```
list object-type documents.abcd
```

Options

You can use these options with the `object-type` component:

- **code**
  Specifies a numeric non-zero code of the application or application host, which is used for troubleshooting and performance reporting. Each application or application host must have a unique code. If not supplied by the user, the code is generated by the system. Use the keyword `generate` to specify that the system generate a new unique code.

- **compression**
  Specifies if this object type supports compression and when it can be enabled. The default value is `disabled`. The possible values are:

  - `disabled`
    Never compresses the response. If you use this option, be aware that it overrides any compression setting configured for the assembly rule.
that the WebAccelerator system matches to the specified object type. You should use this option only if you want the WebAccelerator system to ignore assembly rules for the specified object type.

- **policy-controlled**
  Specifies that compression is controlled by WebAccelerator **policy**. The compression setting is specified in the assembly rule that the WebAccelerator system matched for this object type. In most cases, you should use this option.

- **description**
  Describes the object type.

- **extensions**
  Specifies the extension the WebAccelerator system should find in the file name or Content-Disposition header of the response, in order to match to the specified object type.

- **group**
  Displays the group portion of the name.

- **mime-types**
  Specifies the MIME-types that the WebAccelerator system should find in the Content-Type header of the response, in order to match to the specified object type.

- **name**
  Specifies a unique name for the component. This option is required for the commands **create**, **delete**, and **modify**. The name of the object type must be in form **group.type** where **group** is used to organize object type based on common usage pattern, for example, documents, binary, pages. The type is used to uniquely identify the object type within a group.

- **partition**
  Displays the administrative partition within which the object type resides.

- **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. See **help regex** for a description of regular expression syntax.

**See also**

**create, delete, edit, list, modify, show, tmsh**
policy

Configures an acceleration policy for WebAccelerator.

Module

wam

Syntax

Configure the policy component within the wam module using the syntax shown in the following sections.

Create/Modify

cREATE policy [name]
mODIFY policy [name]
oPTIONS:
  code [integer]
  copy-from [name]
  description [string]
  nodes [add | delete | modify | replace-all-with] {
    [name] {
      options:
        always-proxy [yes | no]
        assembly-compression [enable | disable]
        assembly-compression-ows [enable | disable]
        assembly-css-reorder [enable | disable]
        assembly-css-reorder-cache-size [integer]
        assembly-css-reorder-urls [string ] ...
        assembly-ibr [enable | disable]
        assembly-js-reorder [enable | disable]
        assembly-js-reorder-cache-size [integer]
        assembly-js-reorder-urls [string ] ...
        assembly-minification [enable | disable]
        assembly-multiconnect [enable | disable]
        assembly-on-proxies [enable | disable]
        assembly-pdf-linearization [enable | disable]
        cache-complete-only [enable | disable]
        cache-mode [memory-and-disk | memory-only]
        cache-stand-in-period [integer]
        code [integer]
        defaults-from [name]
        description [string]
jpeg-quality-is-relative [yes | no]
jpeg-quality [integer]
jpeg-strip-exif [no | yes | if-safe | make-safe]
jpeg-sampling factor [preserve | 1x1 | 2x1 | 1x2 | 2x2]
jpeg-progressive-encoding [yes | no]
lifetime-cache-control-extensions
  [add | delete | replace-all-with] {
    [string] ...}
}
lifetime-cache-control-extensions none
lifetime-cache-max-age [integer]
lifetime-honor-ows [yes | no]
lifetime-honor-ows-values
  [add | delete | replace-all-with] {
    [ all-values | no-cache | no-store | no-transform | max-age | must-revalidate | private | proxy-revalidate | s-maxage ] ...}
}
lifetime-honor-ows-values none
lifetime-honor-request [yes | no]
lifetime-honor-request-values
  [add | delete | replace-all-with] {
    [ all-values | no-cache | no-store | no-transform | max-age | max-stale | min-fresh ] ...}
}
lifetime-honor-request-values none
lifetime-http-heuristic [percentage]
lifetime-insert-no-cache [yes | no]
lifetime-preserve-response [yes | no]
lifetime-preserve-response-values
  [add | delete | replace-all-with] {
    [ all-values | no-cache | no-store | no-transform | max-age | must-revalidate | private | proxy-revalidate | s-maxage | custom-extension ] ...}
}
lifetime-preserve-response-values none
lifetime-response-max-age [integer]
lifetime-response-s-maxage [integer]
lifetime-stand-in-codes
  [add | delete | replace-all-with] {
    [HTTP response code] ...}
}
lifetime-stand-in-codes none
lifetime-use-heuristic [yes | no]
options { [hidden | nodelete | nowrite] ...}
order [integer]
response-codes-cached

[add | delete | replace-all-with] {
  [HTTP response code] ...
}

viewstate-cache [yes | no]

viewstate-cache-size [integer]

viewstate-tag [string]

matching [add | modify | delete | replace-all-with] {
  [ host | path | extension | method:[name] | query-param:[name] |
    unnamed-query-param:[name] | path-segment:[name] | cookie:[name] |
    user-agent | referrer | protocol | header:[name] | client-ip | content-type ] {
    options:
    arg-alias [string]
    arg-direction [left-to-right | right-to-left]
    arg-name [string]
    arg-ordinal [number]
    description [string]
    value-case-sensitive [yes | no]
    values [add | modify | delete | replace-all-with] {
      [ [regex] | [string] ] {
        options:
        can-be-empty [yes | no]
        can-be-missing [yes | no]
        invert-match [yes | no]
      }
    }
    values none
  }
  matching none
}

optimize-image [none | to-jpeg | to-gif | to-png | to-tiff]

png-256-colors [yes | no]

variation [add | modify | delete | replace-all-with] {
  [ host | extension | method:[string] | query-param:[name] |
    unnamed-query-param:[name] | path-segment:[name] | cookie:[name] |
    user-agent | referrer | protocol | header:[name] | client-ip ] {
    options:
    arg-alias [string]
    arg-all [yes | no]
    arg-ambiguous-as-unnamed [yes | no]
    arg-direction [left-to-right | right-to-left]
    arg-name [string]
    arg-ordinal [number]
    description [string]
    value-case-sensitive [yes | no]
values [add | modify | delete | replace-all-with] {
  [ [regex] | [string] ] {
    options:
    cache-as [same | different]
    can-be-empty [yes | no]
    can-be-missing [yes | no]
    invert-match [yes | no]
    match-all [yes | no]
  }
  }
values none
}
variation none
[ proxy | proxy-override ]
[add | modify | delete | replace-all-with] {
  [ host | extension | method:[name] | query-param:[name] |
    unnamed-query-param:[name] | path-segment:[name] | cookie:[name] |
    user-agent | referrer | protocol | header:[name] | client-ip ] {
    options:
    arg-alias [string]
    arg-direction [left-to-right | right-to-left]
    arg-name [string]
    arg-ordinal [number]
    description [string]
    value-case-sensitive [yes | no]
    values [add | modify | delete | replace-all-with] {
      [ [regex] | [string] ] {
        options:
        can-be-empty [yes | no]
        can-be-missing [yes | no]
        invert-match [yes | no]
      }
    }
    values none
  }
  }
[ proxy | proxy-override ] none
substitutions [add | modify | delete | replace-all-with] {
  [name] {
    options {
    description [string]
    dst-alias [string]
    dst-direction [left-to-right | right-to-left]
    dst-name [string]
dst-ordinal [number]
dst-type [query-param | unnamed-query-param | path-segment]
dst-url [add | delete | replace-all-with] {
    [URI] ...
}
dst-url none
src-alias [string]
src-direction [left-to-right | right-to-left]
src-name [string]
src-ordinal [number]
src-type
    [ randomizer | request-url | query-param | unnamed-query-param | path-segment ]
src-url [absolute | relative]
}
}
substitutions none
invalidations [add | modify | delete | replace-all-with] {
    [name] {
        options:
        active [yes | no]
        description [string]
        cache-content [add | modify | delete | replace-all-with] {
                options:
                arg-alias [string]
                arg-direction [left-to-right | right-to-left]
                arg-name [string]
                arg-ordinal [number]
                description [string]
                value-case-sensitive [yes | no]
                request-data-alias [string]
                request-data-direction [left-to-right | right-to-left]
                request-data-name [string]
                request-data-ordinal [number]
                request-data-type
                    [ host | path | extension | method | query-param |
                      unnamed-query-param | path-segment | cookie | user-agent |
                      referrer | protocol | header | client-ip ]
                values [add | modify | delete | replace-all-with] {
                    [
                        [regex] | [string] ] {
                        options:
                        can-be-empty [yes | no]
                        can-be-missing [yes | no] 
                    } 
                } 
            } 
        } 
    } 
} 

Traffic Management Shell (tmsh) Reference Guide
invert-match [yes | no]
}
)
)
values none
}
)
)
)
)
partition [name]
publish-build [integer]
publish-comment [string]
published-on [date]

Note
Policies can be created only in the Drafts folder. This is required to support publishing functionality. You can create multiple Drafts folders, one for each folder where published policies are going to reside.

Display
list policy [name ...]
show running-config policy [name ...]
options:
  all-properties
  non-default-properties
  partition
  predefined
  state

Delete

delete policy [name ...]

Save/Load

save policy [name]
load policy [name]
options:
  overwrite
  file [filename]
Publish

\texttt{publish policy [name]}
\begin{itemize}
  \item \texttt{publish-comment [string]}
  \item \texttt{publish-build [integer]}
\end{itemize}

\textbf{\textcolor{red}{Note}}

Published policies can be deleted, but cannot be modified. The only way to update a published policy is to edit and then publish its development version.

Description

You can use the \texttt{policy} component to manage WebAccelerator acceleration policies. An \textit{acceleration policy} is a collection of defined rule parameters that dictate how the WebAccelerator system handles HTTP requests and responses. The WebAccelerator system uses two types of rules to manage content: matching rules and acceleration rules. \textit{Matching rules} are used to classify requests by object type and match the request to a specific acceleration policy. Once matched to an acceleration policy, the WebAccelerator system applies the associated \textit{acceleration rules} to manage the requests and responses. There are multiple types of acceleration rules: variation, proxy, proxy override, parameter value substitution, and invalidation. The WebAccelerator system ships with several predefined acceleration policies that are optimized for specific web applications, in addition to several non-application specific policies for general delivery and one for an optional symmetric deployment.

Examples

\textbf{\textcolor{red}{Note}}

\textit{For the following examples, the current folder is set to /Common.}

Creates a new empty policy named \texttt{My Policy} in the folder /Common/Drafts:
\begin{verbatim}
create policy "Drafts/My Policy"
\end{verbatim}

Creates a new policy \texttt{My Policy} in the folder /Common/Drafts by copying standard system policy /Common/Generic Policy - Complete:
\begin{verbatim}
create policy "Drafts/My Policy" copy-from "/Common/Generic Policy - Complete"
\end{verbatim}

Modifies the policy \texttt{My Policy} by overwriting it with standard system policy /Common/Generic Policy - Complete:
\begin{verbatim}
modify policy "Drafts/My Policy" nodes add ( "My Node" ( default-from Site )}
\end{verbatim}
Chapter 51

Adds a new node **My Node** as the child node of the node **Site**:

```bash
modify policy "Drafts/My Policy" nodes add { "My Node" { default-from Site }}
```

Adds a new matching rule into the node **My Node**. The rule will match content type of the requests to WAM object type **pages.other**:

```bash
modify policy "Drafts/My Policy" nodes modify { "My Node" { matching add { content-type { values add { pages.other }}}} }
```

Publishes the policy **My Policy**:

```bash
publish policy "Drafts/My Policy" publish-comment "Added new node My Node"
```

Deletes the node **My Node** from the policy **My Policy**:

```bash
modify policy "Drafts/My Policy" nodes delete { "My Node" }
```

Deletes the policy **My Policy**:

```bash
delete policy "My Policy"
```

Saves the policy **My Policy** into the file `/var/local/wam/policy.txt`:

```bash
save policy "My Policy" file policy.txt
```

Loads the policy **My Policy** from the file `/tmp/policy.txt` and overwrites the policy if it already exists:

```bash
load policy "Drafts/My Policy" overwrite file /tmp/policy.txt
```

Policy options

You can use these options with the **policy** component:

- **code**
  Specifies a numeric non-zero code of the policy that is used for troubleshooting and performance reporting. Each application or application host must have a unique code. If not supplied by the user, the code is generated by the system. Use the keyword `generate` to specify that the system generate a new unique code.

- **copy-from**
  Specifies the name of an existing policy from which to copy all configuration options. If this field is used in the modify command, the configuration options of the existing policy are replaced with the new ones. The `code`, `state`, `publish-build`, `publish-comment`, and `published-at` options are not updated.

- **description**
  User-defined description of a policy.

- **nodes**
  Specifies the collection of policy nodes. Matching rules and acceleration rules for acceleration policies are organized on the **Policy Tree**, which consists of nodes. The structure of the **Policy Tree** supports a parent-child relationship. This enables you to easily randomize rules. That is, because a leaf node in a **Policy Tree** inherits all the rules from its root node and branch node, you can quickly create multiple leaf nodes that contain the same rule parameters by creating a branch with multiple
leaf nodes. If you override or create new rules at the branch node level, the WebAccelerator system reproduces those changes to the associated leaf nodes.

- **partition**
  Displays the administrative partition within which the policy resides.

- **publish-build**
  Specifies the policy build version that was used during policy publishing. If not specified, this number is automatically incremented by the WebAccelerator system.

- **publish-comment**
  Specifies the user supplied comment that describes the changes in the policy that is being published.

- **published-on**
  Specifies the date and time when this policy was last published.

- **file**
  Specifies the file name where the policy is going to be saved or loaded from. If a full path is not specified, it is set to /var/local/wam directory.

- **overwrite**
  Specifies that the policy file for the `save` command or the policy component for the `load` command can be overwritten if it exists.

### Node options

You can use these options with nodes:

- **always-proxy**
  Specifies that all requests matching this node must be proxied. If enabled, `proxy` rules are not used, even if configured. The `proxy-overide` rules still apply.

- **assembly-compression**
  Specifies, when enabled, that the WebAccelerator system compresses content for responses, using gzip-encoding. Note that to use this feature, you must set the compress value for the response's object type in the corresponding `object-type` component, and the client must be able to accept gzip-encoded content. The default value is `enabled`.

- **assembly-compression-ows**
  Specifies, when enabled, that the WebAccelerator system requests gzip-encoded or deflate-encoded content from the origin web server. Note that the origin web server will comply only if it supports compression, otherwise it will reply with uncompressed content. The default value is `disabled`.

- **assembly-css-reorder**
  Specifies, when enabled, that the WebAccelerator system will reorder CSS URLs to the HEAD section of HTML documents. The CSS URLs that can be reordered are specified using the `assembly-css-reorder-urls` option. The default value is `disabled`.

---

Traffic Management Shell (tmsh) Reference Guide
◆ **assembly-css-reorder-cache-size**
   Specifies the size of the intermediate cache used to store CSS URLs being reordered. Increasing the size of this cache allows more CSS URLs to be reordered. The default value is 32KB.

◆ **assembly-css-reorder-urls**
   Specifies the CSS URLs that can be reordered. The URLs must be fully-qualified, and whitespace used to separate URLs. The URLs must correspond to WebAccelerator URL resources created by the command `create wam resource url`.

◆ **assembly-ibr**
   Specifies, when enabled, that the WebAccelerator system manipulates the web browser cache to reduce requests to your site for relatively static content, such as images and style sheet (CSS) files. The default value is enabled.

◆ **assembly-js-reorder**
   Specifies, when enabled, that the WebAccelerator system will reorder JavaScript URLs to the end of HTML documents. The JavaScript URLs that can be reordered are specified using the `assembly-js-reorder-urls` option. The default value is disabled.

◆ **assembly-js-reorder-cache-size**
   Specifies the size of the intermediate cache used to store JavaScript URLs being reordered. Increasing the size of this cache allows more JavaScript URLs to be reordered. The default value is 32KB.

◆ **assembly-js-reorder-urls**
   Specifies the JavaScript URLs that can be reordered. The URLs must be fully-qualified and whitespace used to separate URLs. The URLs must correspond to WebAccelerator URL resources created by the command `create wam resource url`.

◆ **assembly-minification**
   Specifies, when enabled, that the WebAccelerator system will minify JavaScript and CSS.

◆ **assembly-multiconnect**
   Specifies, when enabled, that the WebAccelerator system modifies embedded URLs with unique sub-domains that prompt the browser to open more persistent connections for each supported protocol (HTTP or HTTPS). To use this feature, you must configure DNS with the additional domains and map those domains to the same IP address as the base origin server. The default value is enabled.

◆ **assembly-on-proxies**
   Specifies, when enabled, that the WebAccelerator system applies the Content Compression and Intelligent Browser Referencing features (if enabled) to content served to clients, even if the content is not served from the WebAccelerator system's cache. Enable this option if you are using the Content Compression or Intelligent Browser Referencing features. The default value is enabled.

◆ **assembly-pdf-linearization**
   Specifies, when enabled, that the WebAccelerator system applies linearization on PDF documents, if the documents match the node
matching rules. PDF linearization transforms the document to include the index of the pages in the beginning. This allows web browsers to load and show specific pages rather than a whole document. See the WebAccelerator documentation for more details. The default value is disabled.

◆ **optimize-image**

Specifies whether image optimization should be applied and the format conversion to use. Each of the four supported formats (JPEG, PNG, GIF, TIFF) can be converted to any of the others. Images using a capability unique to one format can lose that feature when converted to a format that does not support it. (For example, Animated GIFs or multipage-TIFFs will have only the first image when converted to PNG or JPEG). Transparency will be lost when converting from GIF or PNG to JPEG. TIFF is a container for many different image formats so the results will be best-effort and might not list completely.

A converted image will likely have a different number of bytes after conversion. Some conversions are likely to produce fewer bytes; however, a requested conversion will be done even if it results in more bytes (for consistency). For example, you might want to offer multiple formats of an image without storing them all on a server.

A correct Content-Type header will be generated for converted images, but HTML files will not be rewritten.

◆ **jpeg-quality-is-relative**

**jpeg-quality**

JPEG is a lossy compression format. This means when you convert an image to a JPEG and then convert it back, you will not get back exactly the same image you started with. Compression changes the amount of information stored (and therefore the number of bytes), but not the image dimensions (the number of pixels). When **jpeg-quality-is-relative** is set to no, the **jpeg-quality** attribute represents the absolute quality of the JPEG produced. Compression (quality) is represented as a number between 1-100 where 1 is minimal quality, but small, and 100 is high-quality, but large. For most images, useful values of quality will be from about 30-100. Because information once lost cannot be regained, converting a low-quality JPEG to a higher quality is pointless and image optimization will prevent that (by not changing the original to a higher JPEG quality).

You might be unable to choose a specific absolute quality for JPEG images. When **jpeg-quality-is-relative** is set to yes, the relative JPEG quality setting is enabled. In this case, **jpeg-quality** is a percentage (a number between 1-100) that when multiplied by each JPEG's original quality, becomes its optimized quality.

◆ **jpeg-strip-exif**

JPEG files have a header (called EXIF) that contains optional data such as a date, time, camera model, exposure settings, and so on. The EXIF header can also contain a color profile, which is required when included. EXIF headers can be small or large. Unless they contain a color profile,
they do not affect displaying the image, and so can be removed if the loss of the information they contain is acceptable. There are four options for this setting:

- **no**
  Leaves any EXIF headers alone.

- **yes**
  Always strip EXIF headers.

- **if-safe**
  Only strips EXIF headers if they do not have color profiles (ensures that images display properly).

- **make-safe**
  Applies the color profile and then strips the EXIF header (typically decreases image file size). Applying a color profile requires additional CPU time.

- **jpeg-sampling-factor**
  Sets the sampling factor to be used when producing JPEG images. The default value is **preserve**, which matches the original file. You can also explicitly specify this option, as it can sometimes improve compression.

- **jpeg-progressive-encoding**
  When enabled, progressive encoding will be used in JPEG images. For large JPEG files, this can improve compression. When this is enabled, it will be applied only if the file is large enough to improve compression.

- **png-256-colors**
  It is often possible to significantly reduce the size of PNG files without changing their appearance very much by reducing the number of colors to 256 optimally selected values. This optimization is enabled when **png-256-colors** is set to **yes**.

- **cache-complete-only**
  Specifies, when enabled, that the WebAccelerator system caches HTML pages only if the HTML code within the page contains begin and end tags. When disabled, the WebAccelerator system reviews HTTP response headers to determine if the information contained on the page is complete. The default value is **enabled**.

- **cache-mode**
  Specifies where the cached documents will be stored. The default value is **memory-and-disk**. The possible values are:
  
  - **memory-and-disk**
    The cached documents will be stored in memory or on disk.
  
  - **memory-only**
    The cached documents will be stored in memory only.

- **cache-stand-in-period**
  Specifies the amount of time that the WebAccelerator system continues to serve content from the cache if the origin web server does not respond to the WebAccelerator system’s requests for fresh content. The default value is 0 (zero), which means the WebAccelerator system responds to requests for expired content with a HTTP 404 error.
◆ code
Specifies a numeric non-zero code for the node that is used for troubleshooting and performance reporting. All nodes must have unique codes within the policy. If not supplied by the user, the code is generated by the system. Use the keyword `generate` to specify that the system generate a new unique code.

◆ defaults-from
Specifies the node that you want to use as the parent node. Your new node inherits all options and values from the parent node specified. The default value is `none`, which means this is a root node.

◆ description
User-defined description of a node.

◆ invalidations
Specifies the collection of invalidations rules. Invalidations rules enable you to expire cached content before it has reached its time-to-live (TTL) value. This is useful when content updates are event-driven, such as when an item is added to a shopping cart, a request contains a new auction bid, or a poster has submitted content on a forum thread. Invalidations rules can be created only on leaf nodes.

◆ lifetime-cache-control-extensions
Enables you to configure extension tokens to be added to the cache-control header of HTTP response. The WebAccelerator system does not process any of these extensions. It is possible that the origin web server will send cache-control extensions as well. You can choose whether to preserve them by including the custom-extension in the lifetime-preserve-response-values list.

◆ lifetime-cache-max-age
Specifies the amount of time that the WebAccelerator system serves content from the cache before requesting fresh content from the origin web server. The default value is 4 hours.

◆ lifetime-honor-ows
Specifies, if enabled, that the WebAccelerator system honors certain cache-control directives from the origin web server response to determine cache lifetime. The default value is `disabled`.

◆ lifetime-honor-ows-values
Specifies which Cache-Control directive from the origin web server response determines cache lifetime. Available directives are all-values, private, no-cache, no-store, must-revalidate, proxy-revalidate, max-age, s-maxage, and expires. This option is only effective if lifetime-honor-ows is enabled.

◆ lifetime-honor-request
Specifies, if enabled, that the WebAccelerator system honors certain Cache-Control directives from the client's browser request to determine cache lifetime. The default value is `enabled`.

◆ lifetime-honor-request-values
Specifies which cache-control directive from client's browser request will determine cache lifetime. The available directives are all-values,
no-cache, no-store, max-age, max-stale, and min-fresh. This option is only effective if lifetime-honor-request is enabled. The default values are max-age, max-stale, and min-fresh.

- **lifetime-http-heuristic**
  Specifies the percentage, based on the HTTP Last-Modified header, that the WebAccelerator system uses to compute TTL values for cached content. For example, if content was modified 30 days ago and the lifetime-http-heuristic option is set to 50%, the WebAccelerator system caches the content for 15 days. This option is applicable only if you use the HTTP Last-Modified headers to identify content lifetime. The default value is 50%. This option is effective only if lifetime-use-heuristic is enabled.

- **lifetime-insert-no-cache**
  Specifies, when enabled, that the WebAccelerator system inserts a no-cache directive into the HTTP Cache-Control header, which stops the client's browser from locally caching content. This value overrides the HTTP Cache-Control header cache directives sent to the client by the origin web server.

- **lifetime-preserve-response**
  Specifies, if enabled, that the WebAccelerator system preserves certain Cache-Control directives from the origin web server and includes them in the client's browser response. The default value is enabled.

- **lifetime-preserve-response-values**
  Specifies which Cache-Control directive from the origin web server response will be preserved in response to the client's web browser. Available directives are all-values, private, no-cache, no-store, must-revalidate, proxy-revalidate, max-age, s-maxage, expires, and custom-extension. This option is only effective if lifetime-preserve-response is enabled. The default value is all-values.

- **lifetime-response-max-age**
  Specifies, when enabled, the amount of time that the client's browser should locally store content. This value overrides the max-age and expires the directives in the HTTP Cache-Control header that are sent to the client by the origin web server, only if the new value for the max-age is greater than the value supplied by the origin web server. Modify this value only if there is an acceptable trade off between the freshness of the content served to clients and overall site performance.

- **lifetime-response-s-maxage**
  Specifies, when enabled, the amount of time that the client's browser should locally store shared content. This value overrides the s-maxage and expires the directives in the HTTP Cache-Control header that are sent to the client by the origin web server, only if the new value for the s-maxage is greater than the value supplied by the origin web server. Modify this value only if there is an acceptable trade off between the freshness of the shared content served to clients and overall site performance.

- **lifetime-stand-in-codes**
  Specifies that the WebAccelerator system is allowed to serve stale content from the cache if it is not able to re-validate its freshness with the
origin web server. The WebAccelerator system serves invalid content to the downstream proxies or clients if the response code from the origin web server matches one of codes specified with this option. This option is effective only if `cache-stand-in-period` has a non-zero value. The default values are 404, 500, and 504.

◆ **lifetime-use-heuristic**
  Specifies, when enabled, that the WebAccelerator system uses the percentage from `lifetime-use-heuristic` option to compute TTL values for cached content. The default value is no.

◆ **matching**
  Specifies the collection of matching rules. The rules consist of the HTTP request data type parameters that the WebAccelerator system uses to match an incoming HTTP request to a specified node. The following types of HTTP parameters are available for matching rules: host, path, extension, query-param, unnamed-query-param, path-segment, cookie, user-agent, referrer, protocol, method, header, client-ip, and content-type.

◆ **order**
  Specifies the order of the node in the Policy Tree. All nodes in the policy must have an order. The order numbers are sequential, starting from 2. Orders 0 and 1 are reserved for internal use. The child node orders must be greater than the order of their parent node. You can change the order of the nodes by updating the order option of the node that you would like to move. The system honors the specified order if it falls within the range of sibling node orders. Otherwise, the system picks the closest valid order number. The remaining nodes are automatically re-ordered to free requested order number. The node order is also used as a last resort to determine which node to use when multiple nodes match the request. The node with a lower order comes first. New nodes have their order assigned automatically to make them last among their siblings.

◆ **proxy**
  Specifies the collection of proxy rules. In general, proxy rules options are relevant to only requests that match their node, rather than to matched responses. The following types of HTTP parameters are available for proxy rules: host, query-param, unnamed-query-param, path-segment, cookie, user-agent, referrer, protocol, method, header, and client-ip.

◆ **proxy-override**
  Specifies the collection of proxy override rules. You can define proxy override rules and associated conditions under which the WebAccelerator system should ignore proxying rules options. The following types of HTTP parameters are available for proxy override rules: host, query-param, unnamed-query-param, path-segment, cookie, user-agent, referrer, protocol, method, header, and client-ip.

◆ **response-codes-cached**
  Specifies the collection of HTTP response codes that determine whether the WebAccelerator system should cache the content. The valid codes are 300, 301, 302, 307, and 410. The codes 200, 201, 203, and 207 are included in the list implicitly. The default values are 300 and 301.
◆ substitutions
Specifies the collection of parameter value substitution rules. Some requested pages include hyperlinks that require that specific information appear in the response. You can configure parameter value substitution so that when a query parameter contains identification information for a site's visitors, it prompts the WebAccelerator system to serve different content for the request, based on the specific visitor. Conversely, if parameter value substitution is not configured, the WebAccelerator system uses the value that it cached for the original request, for all subsequent requests after the first, even if the subsequent requests have different values that should be used in the response. If you configure parameter value substitution, the WebAccelerator system changes the targeted parameters value on the page served from the cache, so that the parameter you specify appears on the URL embedded in that page.

◆ variation
Specifies the collection of variation rules. When the WebAccelerator system caches responses from the origin web server, it uses certain HTTP request parameters to create a Unique Content Identifier (UCI). The WebAccelerator system stores the UCI in the form of a compiled response and uses the UCI to easily match future requests to the correct content in its cache. You can configure variation rules to add or modify the parameters on which the WebAccelerator system bases its caching process. If the WebAccelerator system receives two requests that are identical except for the value of a query parameter defined in the variation rule, it creates a different UCI for each, and caches each response under its unique UCI. The following types of HTTP parameters are available for variation rules: host, query-param, unnamed-query-param, path-segment, cookie, user-agent, referrer, protocol, method, header, and client-ip. Additionally, you can request case-sensitive matching on variation rules, for example:

```
tmsh modify wam policy Drafts/testdbn nodes add { node1 { matching add { host { values add { rob } value-case-sensitive yes } } } ) ) )
```

◆ viewstate-cache
Specifies, when enabled, that the WebAccelerator system accelerates requests and responses for web form objects that are generated by ASP.NET web applications. Because the file size of forms can be significant, the WebAccelerator system is able to cache and substitute values, thus reducing the file size and achieving faster performance.

◆ viewstate-cache-size
Specifies the size of the ViewState object cache in kilobytes. The default value is 100 kilobytes.

◆ viewstate-tag
Specifies the name of the web form field where the ViewState object is stored. The default value is _VIEWSTATE.
wam Module Components

- **type**
  Displays the node type. The possible types are:
  - **branch**
    The branch nodes exist only for the purpose of propagating rule parameters to leaf nodes. The WebAccelerator system does not perform matching against branch nodes. Branch nodes can have multiple leaf (child) nodes, as well as child branch nodes.
  - **leaf**
    A leaf node inherits rule parameters from its parent branch node. The WebAccelerator system performs matching only against leaf nodes, and then applies the leaf nodes corresponding acceleration rules to the request.

**HTTP parameters**

Both matching and acceleration rules are identified by the type, and optionally, by the name of HTTP parameters that are used inside the rules. The following types of HTTP parameters are available:

- **content-type**
  A rule that uses the content-type parameter is based on type definitions in the object-type components. Unlike the HTTP request data types, a matching rule based on content type is specific to the content type parameter that the WebAccelerator system generates for a response. You specify the regular expression that you want a response's content type to match.

- **client-ip**
  A rule that uses the client IP parameter is based on the IP address of the client making the request. The IP address, however, might not always be the address of the client that originated the request. For example, if the client goes through a proxy server, the IP address is the IP address of the proxy server, rather than the client IP address that originated the request. If several clients use a specific proxy server, they all appear to come from the same IP address.

- **cookie:[name]**
  A rule that uses the cookie parameter is based on a particular cookie that you identify by name, and for which you provide a value to match against. This value is usually literal and must appear on the cookie in the request or in a regular expression that matches the request's cookie that appears on the cookie HTTP request headers. These are the same names you use to set the cookies, using the HTTP Set-Cookie response headers. The HTTP request can contain multiple cookies, and the rule identifier must include the name of the cookie separated with colon (:).

- **extension**
  A rule that uses the extension parameter is based on the value that follows the far-right period, in the far-right segment key of the URL path.

- **header:[name]**
  A rule that uses the header parameter is based on a particular header that you identify by name and for which you provide a value to match.
against. You can use an HTTP request data type header parameter to create rules based on any request header other than one of the recognized HTTP request data types. The HTTP request can contain multiple headers, and the rule identifier must include the name of the header separated with a colon (:).

- **host**
  A rule that uses the host parameter is based on the value provided for the HTTP Host request header field. This header field describes the DNS name that the HTTP request is using.

- **method**
  A rule that uses the method parameter is based on whether the request uses the GET or POST method.

- **query-param:[name]**
  A rule that uses the query parameter is based on a particular query parameter that you identify by name and for which you provide a value to match against. The value is usually literal and must appear on the query parameter in the request, or in a regular expression that matches the requests query parameter value. The query parameter can be in a request that uses GET or POST methods. The HTTP request can contain multiple query parameters, and the rule identifier must include the name of the header separated with colon (:).

- **path**
  A rule that uses the path parameter is based on the path portion of the URI. The path is defined as everything in the URL after the host and up to the end of the URL, or up to the question mark (whichever comes first).

- **path-segment:[name]**
  A segment is the portion of a URI path that is delimited by a forward slash (/). For example, in the path: /apps/search/full/complex.jsp, apps, search, full, and complex.jsp represent path segments. The path can contain multiple segments so the rule identifier must include the name of the segment separated with colon (:). The name can be a segment ordinal or some other string to distinguish it from other segments rules in the same node.

- **protocol**
  A rule that uses the protocol parameter is based on whether the request uses the HTTP or HTTPS protocol.

- **referer**
  A rule that uses the referer parameter is based on the value provided for the HTTP Referer in the request header. (Note the misspelling of Referer. This spelling is defined for this request header in all versions of the HTTP specification.) This header provides the URL location that referred the client to the page that the client is requesting. You do not typically base rules on the Referer request header, unless you want your sites behavior to be dependent on the specific referer. For example, one implementation would be for sites that provide different branding for their pages based on the user's web portal or search engine.
◆ **unnamed-query-param:[name]**
An unnamed query parameter is a query parameter that has no equal sign. That is, only the query parameter value is provided in the URL of the request. The HTTP request can contain multiple unnamed query parameters so the rule identifier must include the name of it separated with colon (:). The name can be the ordinal of unnamed query parameter or some other string that can make it distinguishable from other unnamed query parameter rules in the same node.

◆ **user-agent**
A rule that uses the user agent parameter is based on the value provided for the HTTP User-Agent in the request header, which identifies the browser that sent the request.

**Rule options**

The following rule options are available:

◆ **active**
Specifies, when enabled, that the invalidation trigger rule is enabled. You can use this option to disable a specific invalidation trigger rule temporary, without removing it from the policy.

◆ **arg-all**
Specifies, when enabled, that the rule matches all HTTP parameters of this type rather then one identified by **arg-name** or **arg-ordinal**. This option is applicable to variation rules **query-param**, **unnamed-query-param**, **path-segment**, **cookie**, and **header**. Such rules serve as a fallback case for defining document variation. All root nodes must include one variation rule of each type with this option enabled. The default value is **disabled**.

◆ **arg-alias**
◆ **src-alias**
◆ **dst-alias**
◆ **request-data-alias**
Specifies the user supplied alias for rules that use ordinals to identify HTTP request data. These include the **unnamed-query-param** and **path-segment** rules. The **src-alias** and **dst-alias** options are used in parameter value substitution rules to define aliases for the source and target definitions correspondingly. The **request-data-alias** option defines an alias for the invalidation trigger rules.

◆ **arg-direction**
◆ **src-direction**
◆ **dst-direction**
◆ **request-data-direction**
Specifies the direction that the WebAccelerator system uses to count the ordinal of **path-segment**. The **src-direction** and **dst-direction** options are used in parameter value substitution rules to define the ordinal direction for the source and target definitions correspondingly. The
**request-data-direction** option defines the ordinal direction for the invalidation trigger rules. The default value is **left-to-right**. The possible values are:

- **left-to-right**
  The path segment is counted from left to right.
- **right-to-left**
  The path segment is counted from right to left.

- arg-name
- src-name
- dst-name

- **request-data-name**
  Specifies the name of the parameter type for query-param, cookie, and header. If not specified, **arg-name** option is initialized from the rule name. This option is not effective if **arg-all** is enabled. The **src-name** and **dst-dst** options are used in parameter value substitution rules to define the parameter name for the source and target definitions correspondingly. The **request-data-name** option defines the parameter name for the invalidation trigger rules.

- arg-ordinal
- src-ordinal
- dst-ordinal

- **request-data-ordinal**
  Specifies, in the form of a number, the location of a parameter for unnamed-query-param and path-segment rules. The numbering starts at 1 and follows the direction specified in the corresponding direction option. This option is not effective if **arg-all** is enabled. The **src-ordinal** and **dst-ordinal** options are used in parameter value substitution rules to define the parameter ordinal for the source and target definitions correspondingly. The **request-data-ordinal** option defines the parameter ordinal for the invalidation trigger rules.

- cache-content
  Specifies the parameter for which the WebAccelerator system must obtain fresh content when the invalidations rule is triggered. The available request types are: host, path, extension, query-param, unnamed-query-param, path-segment, cookie, user-agent, referrer, protocol, method, header, and client-ip.

  *Note:* You must select and configure the path parameter for the cached content to invalidate, or the invalidations rule will fail to trigger. All other parameters are optional.

- description
  User-defined description of a rule.

- dst-type
  Specifies the HTTP parameter type to use as a target definition for the request value substitution rule. A target definition contains a value in the embedded URL that you want the WebAccelerator system to replace with the value that you specified for the source definition, during assembly.
The possible values are:

- **path-segment**
  Specifies that the WebAccelerator system targets the URL parameter, as specified by the `dst-ordinal` and `dst-direction` you define.

- **query-param**
  Specifies that the WebAccelerator system targets the URL parameter, as specified by the `dst-name` you define.

- **unnamed-query-param**
  Specifies that the WebAccelerator system substitutes the URL parameter, as specified by the `dst-ordinal` you define.

- **dst-urls**
  Specifies the collection of URLs in the request for which you want the WebAccelerator system to replace content.

- **request**
  Specifies a parameter in the request that triggers the invalidations rule. The available request types are: `host`, `path`, `extension`, `query-param`, `unnamed-query-param`, `path-segment`, `cookie`, `user-agent`, `referrer`, `protocol`, `method`, `header`, and `client-ip`.

  *Note:* You must select and configure the `path` parameter for the `request` header criteria, or the invalidations rule will fail to trigger. All other parameters are optional.

- **request-data-type**
  Specifies the HTTP request parameter value that the WebAccelerator system should find in its cache and for which it should request updated content from the origin web server. The default value is `undefined`. The following types of HTTP parameters are available:

  - **host**
  - **query-param**
  - **unnamed-query-param**
  - **path-segment**
  - **cookie**
  - **user-agent**
  - **referrer**
  - **header**
  - **client-ip**

  Specifies that the WebAccelerator system should use the corresponding value from the request that triggered the invalidation.

  Additional data, if required to identify the value, must be specified in the `request-data-name`, `request-data-ordinal`, and `request-data-direction` options. The `values` option is ignored.

- **undefined**
  Specifies that the WebAccelerator system should not use any values from the request that triggered the invalidation. You must add a value into the `values` option with which to compare the cached content.
- **src-type**
  Specifies the HTTP parameter type to use as source definition for the request value substitution rule. A source definition contains the value that the WebAccelerator system embeds in the URL, in place of the cached (target definition) value, during substitution. Typically, the source definition is a specific request element, such as a particular query parameter; however, you can specify another source type, such as a random number. The possible values are:
  - **path-segment**
    Specifies that the WebAccelerator system substitutes the URL parameter, as specified by the `src-ordinal` and `src-direction` options you define.
  - **query-param**
    Specifies that the WebAccelerator system substitutes the URL parameter, as specified by the `src-name` option you define.
  - **randomizer**
    Specifies that the WebAccelerator system generates a random number and places that number on the targeted location in an embedded URL.
  - **request-url**
    Specifies that the WebAccelerator system is limited to target-specific URLs embedded in a page, as defined in the prefix that an embedded URL must match before the WebAccelerator system performs substitution. If you use the request URL as the source, the WebAccelerator system uses the entire request URL as the value to substitute.
  - **unnamed-query-param**
    Specifies that the WebAccelerator system substitutes the URL parameter, as specified by the `src-ordinal` option you define.
- **src-url**
  Specifies whether the request URL is a relative URL or an absolute URL. The default value is absolute.
- **value-case-sensitive**
  Specifies, when enabled, that the HTTP parameter must be matched against supplied value(s) in a case-sensitive manner. The default value is no.
- **values**
  Values are a collection of rule parameters that enable you to specify different parameter values for the same rule. Most rules allow only one value, while variation rules support multiple values. Each value can prompt a different behavior by the WebAccelerator system. All variation rules must include at least one value with the `match-all` option enabled. A value can be represented by actual string, regex, or multiple strings, or regexes separated by a space ( ).
Rule value options

The following rule value options are available:

- **can-be-empty**
  Specifies, when enabled, that the defined HTTP request parameter is included in the request, but has no value (is an empty string). The default value is **no**.

- **can-be-missing**
  Specifies, when enabled, that the defined HTTP request parameter is absent from the request. The default value is **no**.

- **invert-match**
  Specifies, when enabled, that the defined HTTP request parameter does not match the associated regular expression that you defined. The default value is **no**.

- **match-all**
  Specifies, when enabled, that the defined HTTP request parameter matches all possible values. This option is available only for variation rule values as a fallback case. Each variation rule must have at least one value with this option enabled. The default value is **no**.

- **cache-as**
  Specifies whether the associated value should prompt the WebAccelerator system to reply to matched requests with the same or different content. This option is available only for variation rule values.

See also

create, delete, edit, list, modify, show, tmsh
wom Module Components

- Introducing the wom module
- Alphabetical list of components
Introducing the wom module

You can use the `tmsh` components that reside within the `wom` module to configure WAN optimization. For more information about the `tmsh` hierarchical structure, see Chapter 2, Understanding and Using the Traffic Management Shell.

Alphabetical list of components

The remainder of this chapter lists the `tmsh` components that are available in the `wom` module.
advertised-route

Configures a route advertised by the local endpoint to remote endpoints for WAN optimization.

Module

wom

Syntax

Configure the advertised-route component within the wom module using the following syntax.

Create/Modify

create advertised-route [ip address/netmask]
modify advertised-route [ip address/netmask | all]

options:

description [string]
dest [ip address/netmask]
include [disabled | enabled]
label [value]
metric [integer]
origin [configured | discovered | manually-saved | persistable]

Display

list advertised-route
show advertised-route

options:

all
all-properties
app-service
running-config
non-default properties
one-line

Delete

delete advertised-route [name]
Description

You can use the `advertised-route` component to configure a subnet that the system can reach through the local endpoint. You can specify a netmask or use slash format.

Routes are advertised to all connected WAN Optimization Managers. The remote endpoints use the subnet configuration information to determine peer routing and optimization actions.

Examples

Displays all endpoint advertised routes for the local WAN Optimization Manager™:

```
list advertised-route all
```

Deletes the advertised route `adv_rt2`:

```
delete advertised-route adv_rt2
```

Options

You can use these options with the `advertised-route` component:

- **app-service**
  Displays the application service to which the object belongs. The default value is `none`.

  **Note:** If the `strict-updates` option is enabled on the Application Service that owns the object, you cannot modify or delete the object. Only the Application Service can modify or delete the object.

- **description**
  User-defined description.

- **dest**
  Specifies the IP address and netmask of the advertised route.

- **include**
  Enables or disables the inclusion of this route in the optimization of traffic. This option allows you to define a subset of IP addresses to exclude from optimization within a larger included subnet. An excluded endpoint advertised route must be a valid address range subset of an included endpoint advertised route.

- **label**
  Specifies an optional descriptive label for this route.

- **metric**
  Specifies a routing number to select between WAN Optimization Manager pairs. The higher the number, the more expensive the route in terms of resources. Not implemented in this release.

- **origin**
  Specifies whether the route was discovered automatically or configured manually. You can change the origin from `discovered` to `persistable`, if
you want to save the route to the file `bigip_local.conf` when you use the command `save config`. After you run the command `save config`, this attribute changes to `manually saved`. Endpoints that have the attribute `discovered` are not saved to the file `bigip_local.conf`.

The options are:

- **configured**
  Indicates that you manually configured this route. The system automatically sets this value, and you cannot change it.

- **discovered**
  Indicates that the system automatically discovered this route. Note that routes for which the value of the `origin` property is `discovered` are not saved to the file `bigip_local.conf`.

- **manually-saved**
  After you run the command `save /sys config`, the value of the `origin` property that was set to `persistable` changes to `manually-saved`. Note that after the system changes the value to `manually-saved`, you cannot change it again.

- **persistable**
  Change the origin from `discovered` to `persistable`, if you want to save the route to the file `bigip_local.conf` when you use the command `save /sys config`.

**See also**

`create`, `delete`, `list`, `modify`, `show`, `tmsh`, `wom local-endpoint`, `wom remote-endpoint`, `wom server-discovery`
**deduplication**

Configures symmetric data deduplication for WAN optimization.

**Module**

**wom**

**Syntax**

Configure the `deduplication` component within the `wom` module using the following syntax.

**Modify**

```plaintext
modify deduplication
  options:
    codec [sdd-v2| sdd-v3]
    [disabled | enabled]
    max-endpoint-count [integer]
```

**Display**

```plaintext
list deduplication
show running-config deduplication
  options:
    dictionary-size
    one-line
```

**Description**

You can use the `deduplication` component to configure symmetric data deduplication, which compresses data over the WAN by identifying and removing repetitive data patterns.

**Examples**

Displays all the deduplication settings:

```plaintext
list deduplication all-properties
```

Sets the maximum number of remote endpoints to **4**:

```plaintext
modify deduplication max-endpoint-count 4
```
Options

You can use these options with the `deduplication` component:

- **codec**
  Specifies which algorithm the system uses for deduplication. The default value is `sdd-v2`.
  The options are:
  
  - **sdd-v2**
    Used for low number of spokes, such as for data center to data center connections.
  
  - **sdd-v3**
    Used for high number of spokes, such as for connecting remote sites and mesh topologies.

- **dictionary-size**
  Displays the current size of the dictionary, which deduplication uses to look up byte patterns.

- **[disabled | enabled]**
  Enables or disables deduplication. The default value is `enabled`.

- **max-endpoint-count**
  Specifies the maximum number of concurrent remote endpoints supported by symmetric data deduplication. The valid range for codec `sdd-v2` is from 1 through 64. The default value for `sdd-v2` is 1. For codec `sdd-v3`, the maximum endpoint count is set to a default value of 128.

See also

- list, modify, show, sys datastor, tmsh, wom profile isession
diagnose-conn

Diagnoses network connection problems.

Module

wom

Syntax

run diagnose-conn

Description

You can use the diagnose-conn component within the wom module to display diagnostic information about network connections.

See also

run, tmsh, wom verify-config
endpoint-discovery

Configures automatic discovery of remote endpoints for WAN optimization.

Module

wom

Syntax

Configure the endpoint-discovery component within the wom module using the following syntax.

Modify

```
modify endpoint-discovery
options:
  auto-save [disabled | enabled]
  description [string]
  discoverable [disabled | enabled]
  discovered-endpoint [disabled | enabled]
  icmp-max-requests [integer]
  icmp-min-backoff [integer]
  icmp-num-retries [integer]
  max-endpoint-count [integer]
  mode [disable | enable-all | enable-icmp | enable-tcp]
reset-stats endpoint-discovery
```

Display

```
list endpoint-discovery
show running-config endpoint-discovery
options:
  all-properties
  non-default-properties
  one-line
show endpoint-discovery
options:
  (default | exa | gig | kil | meg | peta | raw | tera | yotta | zetta)
```
Description

You can use the endpoint-discovery component to specify parameters for automatically discovering remote endpoints for WAN optimization. These endpoints are configured WAN Optimization Managers on remote BIG-IP® systems that advertise themselves to the configured WAN Optimization Manager™ on the local BIG-IP system.

Examples

Limits the number of remote endpoints that can be discovered to ten. After discovering ten remote endpoints, the WOM stops sending probe messages:

```
modify endpoint-discovery max-endpoint-count 10
```

Displays the configuration parameters for the discovery of remote endpoints:

```
list endpoint-discovery all-properties
```

Options

You can use these options with the endpoint-discovery component:

- **auto-save**
  
  Specifies whether the system automatically saves remote endpoints that it discovers. The default value is enabled.

- **description**
  
  User-defined description.

- **discoverable**
  
  Specifies whether the WAN Optimization Manager responds to probe messages it receives from WAN Optimization Managers on remote BIG-IP systems. The default value is enabled.

- **discovered-endpoint**
  
  Specifies whether the WAN Optimization Manager sends out probe messages to discover other WAN Optimization Managers on remote BIG-IP systems in the network. The default value is enabled.

- **icmp-max-requests**
  
  Specifies the maximum number of ICMP probe message requests, after which the system stops sending probe message requests until at least one message is cleared from the queue by either a timeout or a response. The default value is 1024.

- **icmp-min-backoff**
  
  Specifies the maximum number of times the system sends an ICMP probe message request for a single flow. The range is from 0 to 255. The default value is 5.
◆ icmp-num-retries
Specifies the maximum number of times the system sends an ICMP probe message request for a single flow. The range is from 0 to 255. The default value is 5.

◆ max-endpoint-count
Specifies the highest number of remote endpoints for the system to discover before it stops sending probe messages. The range is from 0 to 255. The default value is 0, which indicates no limit.

◆ mode
Specifies the type of probe messages the system should send. The default value is enable-all.
The options are:
  • disable
    Turns off probe messages.
  • enable-icmp
    Sends only ICMP probe messages.
  • enable-tcp
    Sends only TCP probe messages.
  • enable-all
    Sends both ICMP and TCP probe messages.

See also

list, modify, show, tmsh, wom local-endpoint, wom remote-endpoint, wom server-discovery
**local-endpoint**

Configures the local endpoint for the WAN Optimization Manager.

**Module**

`wom`

**Syntax**

Configure the `local-endpoint` component within the `wom` module using the following syntax.

**Modify**

```plaintext
modify local-endpoint
options:
    addresses [add | delete | replace-all-with] {
        [ip address]
    }
    addresses none
    allow-nat [disabled | enabled]
    description [string]
    endpoint [disabled | enabled]
    ip-encap-mtu [unsigned integer]
    ip-encap-profile [none | profile name]
    ip-encap-type [gre | ipip | ipsec | none]
    no-route [drop | passthru]
    server-ssl [profile name]
    snat [local | none | remote]
    tunnel-port [unsigned integer]
```

**Display**

```plaintext
list local-endpoint
show local-endpoint
show running-config local-endpoint
    options:
        all-properties
        non-default-properties
        one-line
```

**Delete**

```plaintext
delete local-endpoint
```
Description

You can use the **local-endpoint** component to modify the settings for the local endpoint for the WAN Optimization Manager on the local BIG-IP system.

Examples

Disables the **allow-nat** option, specifying that the system does not accept connections for traffic behind a Network Address Translation (NAT) device:

```
modify local-endpoint allow-nat disabled
```

Displays all of the properties of the **local-endpoint** component:

```
list local-endpoint all-properties
```

Options

You can use these options with the **local-endpoint** component:

- **addresses**
  Specifies a single IP address the system uses for the local endpoint. The IP address must be in the same subnet as a self IP address on the BIG-IP system.

- **allow-nat**
  When enabled, specifies that the system accepts connections for traffic behind a Network Address Translation device. The default value is **enabled**.

- **description**
  User-defined description.

- **endpoint**
  When enabled, specifies that the local endpoint is available for initiating and receiving optimized traffic. The default value is **enabled**.
  To turn off WAN optimization on this endpoint, use **disabled**.

- **ip-encap-mtu**
  Specifies the maximum transfer unit for IP encapsulated traffic.

- **ip-encap-profile**
  Specifies the name of the profile with the encapsulation settings. This profile must be of the type specified for the setting **ip-encap-type**.

- **ip-encap-type**
  Specifies the type of IP layer encapsulation to perform on iSession™ traffic. The default value is **none**.
  The options are:
  - **gre**
    The system uses the Generic Routing Encapsulation (GRE) tunneling protocol.
• **ipip**
  The system uses the IP over IP (IPIP) tunneling protocol.

• **ipsec**
  The system uses IP security (IPsec) encapsulation.

• **none**
  No IP encapsulation takes place.

◆ **no-route**
  Specifies what the system does with traffic for which there is no remote
  endpoint to complete the iSession connection. The default value is
  *passthru*.

  The options are:

  • **drop**
    The system terminates the traffic flow.

  • **passthru**
    The traffic flow continues without an iSession connection.

◆ **server-ssl**
  Specifies the default Server SSL profile the system uses for
  authentication. The default value is *server-ssl*.

◆ **snat**
  Specifies the IP address the system uses for incoming traffic as the source
  IP address of the TCP connection between the WAN Optimization
  Manager and the server. The default value is *none*.

  The options are:

  • **local**
    The system uses the endpoint IP address closest to the destination.
    Use this setting to make sure the return route also goes through the
    BIG-IP system, so that both sides of the connection can be optimized.
    This setting is useful if responses returning from the server to the
    client would not normally pass through the BIG-IP system.

  • **none**
    The system uses the original connecting client IP address.

  • **remote**
    The system uses the source IP address of the incoming iSession
    connection. Use this setting when an appliance that uses NAT is
    located between the WAN Optimization endpoints.

◆ **tunnel-port**
  Specifies the number of the port on the local endpoint that the WAN
  Optimization Manager uses for control connections. The port must have
  access through the firewall. The valid range is from 1 through 65535.
  The default value is 443.

**See also**

- list, modify, show, tmsh, wom advertised-route, wom remote-endpoint
remote-endpoint

Configures one or more remote endpoints for the WAN Optimization Manager.

Module

wom

Syntax

Configure the remote-endpoint component within the wom module using the following syntax.

Create/Modify

create remote-endpoint [name]
modyf remote-endpoint [name]
  options:
    address [ip address]
    allow-routing [disabled | enabled]
    dedup-action [none | cache-refresh]
    endpoint [disabled | enabled]
    ip-encap-mtu [unsigned integer]
    ip-encap-profile [none | profile name]
    ip-encap-type [default | gre | ipip | ipsec | none]
    origin [configured | discovered | manually-saved | persistable]
    server-ssl [profile name]
    snat [default | local | none | remote]
    tunnel-encrypt [disabled | enabled]
    tunnel-port [unsigned integer]
  reset-stats remote-endpoint

Display

list remote-endpoint
list remote-endpoint [name]
show running-config remote-endpoint
show running-config remote-endpoint [name]
  options:
    all-properties
    dedup-codec
    non-default-properties
    one-line
  show remote-endpoint
show remote-endpoint [ip address]

options:
  (default | exa | gig | kil | meg | peta | raw | tera | yotta | zetta)

Delete

delete remote-endpoint [name]

◆ Note
If you delete a remote endpoint without also disabling the endpoint-discovery component, the remote endpoint can reappear as it is rediscovered. To remove a remote endpoint from traffic initiated by this WAN Optimization Manager, set the endpoint option of the remote-endpoint component to disabled.

Description

You can use the remote-endpoint component to create, modify, or delete a remote endpoint for traffic from the local WAN Optimization Manager.

Examples

Disables the WAN optimization connection to the remote endpoint that has the IP address of 13.16.0.5:

modify remote-endpoint remote 13.16.0.5 disabled

Displays all the properties of all the remote endpoints for traffic from the local WAN Optimization Manager:

list remote-endpoint all-properties

Options

You can use these options with the remote-endpoint component:

◆ allow-routing
  Specifies whether there is a route from the local endpoint to this remote endpoint through which the local endpoint can establish connections. The default value is enabled.

◆ address
  Specifies the IP address of the remote endpoint.

◆ dedup-action
  Clears the cache used for symmetric data deduplication on the specified remote endpoint and immediately resets the value to none.
◆ dedup-codec
Displays the deduplication codec used by the remote endpoint: sdd-v2 or sdd-v3.

◆ endpoint
When enabled, specifies that traffic can be optimized between the local and remote endpoints. The default value is enabled.

*Note:* Disabling a remote endpoint affects only the connection between the local endpoint and this remote endpoint.

◆ ip-encap-mtu
Specifies the maximum transfer unit for IP encapsulated traffic. The default value is 0.

◆ ip-encap-profile
Specifies the name of a profile with encapsulation settings. This profile must be of the type specified for the setting ip-encap-type.

◆ ip-encap-type
Specifies the type of IP layer encapsulation performed on iSession traffic. The default value is default.

The options are:

* • default
  The system uses the ip-encap-type value set for the local endpoint.

* • gre
  The system uses the Generic Routing Encapsulation (GRE) tunneling protocol.

* • ipip
  The system uses the IP over IP (IPIP) tunneling protocol.

* • ipsec
  The system uses IP security (IPsec) encapsulation.

* • none
  No IP encapsulation takes place.

◆ origin
Specifies whether the remote endpoint was discovered automatically or configured manually. You can change the origin from discovered to persistable, if you want to save the endpoint to the file bigip_local.conf when you use the save / sys config command. After you run the save / sys config command, this attribute changes to manually-saved.

Endpoints that have the attribute discovered are not saved to the file bigip_local.conf.

The options are:

* • configured
  Indicates that you manually configured this remote endpoint. The system automatically sets this value, and you cannot change it.

* • discovered
  Indicates that the system automatically discovered this remote endpoint. Note that endpoints for which the value of the origin property is discovered are not saved to the file bigip_local.conf.
manually-saved
After you run the save / sys config command, the value of the origin property that was set to persistable changes to manually-saved. Note that after the system changes the value to manually-saved, you cannot change it again.

persistable
Change the origin from discovered to persistable, if you want to save the endpoint to the file bigip_local.conf when you use the save / sys config command.

server-ssl
Specifies the Server SSL profile the system uses to connect to this remote endpoint. This setting overrides the server-ssl setting for the local-endpoint component.

snat
Specifies the IP address the system uses as the source IP address of the TCP connection between the WAN Optimization Manager and the server. The default value is none.

The options are:

• default
  The system uses the snat value set for the local-endpoint component.

• local
  The system uses the endpoint IP address closest to the destination. Use this setting to make sure the return route also goes through the BIG-IP system, so that both sides of the connection can be optimized. This setting is useful if responses returning from the server to the client would not normally pass through the BIG-IP system.

• none
  The system uses the original connecting client IP address.

• remote
  The system uses the source IP address of the incoming iSession connection. Use this setting when an appliance that uses NAT is located between the WAN Optimization Manager endpoints.

tunnel-encrypt
Enables or disables encryption of traffic passing between the two WAN Optimization Managers. The default value is enabled.

tunnel-port
Specifies whether to use a specific port for traffic optimized to this endpoint or to use port transparency (0). The default value is 443.

See also
create, delete, list, modify, show, tmsh, wom advertised-route, wom local-endpoint
remote-route

Displays the destination routes learned from the remote endpoints.

Module

wom

Syntax

show remote-route

options:
(default | exa | gig | kil | meg | peta | raw | tera | yotta | zetta)
detail

Description

You can use the remote-route component within the wom module to view the subnets that the system can reach through the remote endpoint(s). The system can optimize traffic destined for these subnets.

Examples

Displays the subnets reachable through the remote endpoint(s) configured on the WAN Optimization Manager:
show remote-route

Displays detailed information about the remote endpoint(s) through which the displayed subnets can be reached:
show remote-route detail

See also

show, tmsh, wom advertised-route, wom remote-endpoint, wom server-discovery
server-discovery

Configures the dynamic discovery of servers that can be reached through the local endpoint and the routes to reach them.

Module

wom

Syntax

Configure the server-discovery component within the wom module using the following syntax.

Modify

modify server-discovery

options:
  auto-save [disabled | enabled]
  description [string]
  filter-mode [exclude | include]
  idle-time-limit [integer]
  ip-ttl-limit [integer]
  max-server-count [integer]
  min-idle-time [integer]
  min-prefix-length-ipv4 [integer]
  min-prefix-length-ipv6 [integer]
  mode [disabled | enabled]
  rtt-threshold [integer]
  subnet-filter [add | delete | none | replace-all-with] {
    [ip address]
  }
  time-unit [days | hours | minutes]

Display

list server-discovery
show running-config server-discovery

options:
  all-properties
  auto-save
  current-module
  description
  filter-mode
  idle-time-limit
Description

You can use the server-discovery component to configure the dynamic discovery of servers and the routes to reach them through the local endpoint. The local endpoint advertises these routes to any remote endpoints to which it is connected.

Examples

Displays the settings for dynamic discovery of advertised routes:

```
list server-discovery all-properties
```

Disables the dynamic discovery of advertised routes:

```
modify server-discovery mode disabled
```

Options

You can use these options with the server-discovery component:

- **auto-save**
  Specifies whether the system automatically saves the subnets that it discovers that can be reached through the local endpoint. The default value is enabled.

- **filter-mode**
  Specifies whether the subnets you add using the attribute subnet-filter are excluded from or included in the discovery of advertised routes. If you specify include and do not specify any IP addresses, no subnets are discovered. The default value is exclude with no IP addresses specified, which means that all advertised routes that conform to the specified attributes are discovered.
- **idle-time-limit**
  Specifies the maximum length of time a route can be idle without being removed from discovery. The default value is 0. Use the attribute `time-unit` to set the unit of measure. Use the attribute `min-idle-time` to set the minimum length of idle time.

- **ip-ttl-limit**
  Specifies the number of network segments on which a packet is allowed to travel before the route is removed from discovery. The more routers a packet travels through, the smaller the `ip-ttl-limit` value is. The range is 0 to 255. The default value is 5.

- **max-server-count**
  Specifies the highest number of servers the system discovers before it stops looking. The default value is 50.

- **min-idle-time**
  Specifies the minimum length of time a route must be idle before being removed from discovery. The default value is 0, which indicates that idle time is not considered in discovery. Use the attribute `time-unit` to set the unit of measure. Use the attribute `idle-time-limit` to set the maximum length of idle time.

- **min-prefix-length-ipv4**
  Specifies the minimum prefix length for route aggregation in IPV4 networks. The range is 0 to 32. The default value is 32.

- **min-prefix-length-ipv6**
  Specifies the minimum prefix length for route aggregation in IPV6 networks. The range is 0 to 128. The default value is 128.

- **mode**
  Enables or disables the dynamic discovery of servers that can be reached through the local endpoint. For server discovery to take place, the setting `mode` of the component `wom endpoint-discovery` must not be set to disabled.

- **rtt-threshold**
  Specifies that the system does not add servers it discovers with a round-trip time greater than this value, in milliseconds. The default value is 10.

- **subnet-filter**
  Specifies the IP addresses of the subnets to include in or exclude from the discovery of advertised routes, depending on the setting you selected for the attribute `filter-mode`. The default value is `none`. If you selected `include` for the attribute `filter-mode`, and do not specify any IP addresses, no subnets are discovered.

- **time-unit**
  Specifies the unit of measure (days, hours, or minutes) for the length of idle time specified using the attributes `idle-time-limit` and `min-idle-time`. 


See also

list, modify, show, tmsh, wom advertised-route, wom endpoint-discovery, wom local-endpoint, wom remote-route
verify-config

Checks the WAN Optimization Manager configuration.

Module

wom

Syntax

run verify-config

Description

You can use the verify-config component within the wom module to display configuration information about the WAN Optimization Manager that can be used for troubleshooting.

See also

run, tmsh, wom diagnose-conn
wom profile Module Components

• Introducing the wom profile module

• Alphabetical list of components
Introducing the wom profile module

You can use the \texttt{tmsh} components that reside within the \texttt{wom profile} module to configure profiles for WAN optimization. For more information about the \texttt{tmsh} hierarchical structure, see Chapter 2, \textit{Understanding and Using the Traffic Management Shell}.

Alphabetical list of components

The remainder of this chapter lists the \texttt{tmsh} components that are available in the \texttt{wom profile} module.
cifs

Configures a Common Internet File System (CIFS) profile.

Module

wom profile

Syntax

Configure the cifs component within the wom profile module using the following syntax.

Create/Modify

create cifs [name]
modify cifs [name]

options:
  defaults-from [ [name] | none]
  description [string]
  fast-close [disabled | enabled]
  fast-set-file-info [disabled | enabled]
  office-2003-extended [disabled | enabled]
  read-ahead [disabled | enabled]
  record-replay [disabled | enabled]
  write-behind [disabled | enabled]

Display

list cifs
list cifs [ [name] [glob] [regex] ... ]
show running-config cifs
show running-config cifs [ [name] [glob] [regex] ... ]

options:
  all-properties
  app-service
  non-default-properties
  one-line
  partition
show cifs
show cifs [ [name] [glob] [regex] ... ]

options:
  (default | exa | gig | kil | meg | peta | raw | tera | yotta | zetta)
Delete

```
delete cifs [name]
```

Description

You can use the `cifs` component to manage a CIFS profile.

Examples

Creates a CIFS profile named `my_cifs_profile` using the system defaults:

```
create cifs my_cifs_profile
```

Turns off `fast-close` for the CIFS profile named `my_cifs_profile`:

```
modify cifs my_cifs_profile fast-close disabled
```

Options

You can use these options with the `cifs` component:

- **app-service**
  Displays the application service to which the object belongs. The default value is `none`.

  *Note: If the strict-updates option is enabled on the Application Service that owns the object, you cannot modify or delete the object. Only the Application Service can modify or delete the object.*

- **defaults-from**
  Specifies the profile that you want to use as the parent profile. Your new profile inherits all settings and values from the parent profile specified. The default value is `cifs`.

- **description**
  User-defined description.

- **fast-close**
  Specifies whether the system speeds up file close operations by fulfilling them through the WAN Optimization Manager™ closer to the request initiator. The default value is `enabled`.

- **fast-set-file-info**
  Specifies whether the system speeds up file metadata change requests by fulfilling the requests through the WAN Optimization Manager closer to the request initiator. The default value is `enabled`.

- **glob**
  Displays the items that match the `glob` expression. For a description of `glob` expression syntax, see the `glob` man page.

- **name**
  Specifies a unique name for the component. This option is required for the commands `create`, `delete`, and `modify`.
◆ **office-2003-extended**
  Specifies whether the system performs read-ahead operations based on parsing the Microsoft CDF file and understanding its structure. The default value is **enabled**.

◆ **partition**
  Displays the administrative partition within which the component resides.

◆ **read-ahead**
  Specifies whether the system speeds up CIFS file downloads by prefetching the file data on the WAN Optimization Manager closer to the request initiator. The default value is **enabled**.

◆ **record-replay**
  Specifies whether the system opens CIFS files faster by performing more intelligent read-ahead operations. The default value is **enabled**.

◆ **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. For a description of regular expression syntax, see the **regex** man page.

◆ **write-behind**
  Specifies whether the system speeds up CIFS file uploads to the server by fulfilling write requests through the WAN Optimization Manager closer to the request initiator. The default value is **enabled**.

See also

create, delete, glob, list, ltm virtual, modify, regex, show, tmsh
**isession**

Configures an iSession™ profile.

**Module**

**wom profile**

**Syntax**

Configure the **isession** component within the **wom profile** module using the following syntax.

**Create/Modify**

```plaintext
create isession [name]
modify isession [name]
```

options:

- adaptive-compression [disabled | enabled]
- compression [disabled | enabled]
- compression-codecs [add | delete | none | replace-all-with] {
  options:
  - bzip2
  - deflate
  - lzo
}
- data-encryption [disabled | enabled]
- deduplication [disabled | enabled]
- defaults-from [ [name] | none]
- deflate-compression-level [integer]
- description [string]
- mode [disabled | enabled]
- port-transparency [disabled | enabled]
- reuse-connection [disabled | enabled]
- target-virtual [none | host-match-all | host-match-no-isession | virtual-match-all]

**reset-stats isession**

**Display**

```plaintext
list isession
list isession [ [name] | [glob] | [regex] ] ... ]
show running-config isession
show running-config isession [ [name] | [glob] | [regex] ] ... ]
```
Chapter 53

options:
  all-properties
  app-service
  non-default-properties
  one-line
  partition

show isession

show isession [ [name] | [glob] | [regex] ] ... ]

options:
  (default | exa | gig | kil | meg | peta | raw | tera | yotta | zetta)
  field-fmt
  global

Delete

delete isession [name]

Description

You can use the isession component to manage an iSession profile.

Examples

Creates an iSession profile named my_isession_profile using the system defaults:

create isession my_isession_profile defaults-from isession

Turns off deduplication for the iSession profile named my_isession_profile:

modify isession my_isession_profile deduplication disabled

Options

You can use these options with the isession component:

- **adaptive-compression**
  Enables or disables the automatic selection of the optimal compression algorithm for the current traffic, based on link speed. The system can use only compression algorithms that are enabled. To establish and maintain the connection, you must enable at least one compression setting. The default value is enabled.

- **app-service**
  Displays the application service to which the object belongs. The default value is none.

  Note: If the strict-updates option is enabled on the Application Service that owns the object, you cannot modify or delete the object. Only the Application Service can modify or delete the object.
◆ **compression**
   Enables or disables the compression of data according to the methods you select for the attribute **compression-codecs**. The default value is **enabled**.

◆ **compression-codecs**
   Specifies the codecs to use for compression. The following codecs are available:
   - **bzip2**
     Specifies the use of the bzip2 compression algorithm, which improves compression ratios on low-bandwidth data links.
   - **deflate**
     Specifies the use of the Deflate data compression algorithm.
   - **lzo**
     Specifies the use of the Lempel-Ziv-Oberhumer (LZO) data compression algorithm.

◆ **data-encryption**
   Enables or disables encryption of the traffic on the outbound connection. If you select **enabled**, the system uses the SSL profiles specified on the local and remote endpoints of the iSession connection. The default value is **disabled**.

◆ **deduplication**
   Enables or disables data deduplication, which replaces previously transmitted data with references.

◆ **defaults-from**
   Specifies the profile that you want to use as the parent profile. Your new profile inherits all settings and values from the parent profile specified. The default value is **isession**.

◆ **deflate-compression-level**
   Specifies the level of compression, if deflate-compression is enabled and adaptive-compression is disabled. The range is 1 to 9. A higher value causes the CPU to spend more time looking for matches, which can result in better compression. The default value is 1.

◆ **description**
   User-defined description.

◆ **glob**
   Displays the items that match the **glob** expression. For a description of **glob** expression syntax, see the **glob** man page.

◆ **mode**
   Enables or disables the use of this profile for WAN optimization traffic. The default value is **enabled**.

◆ **name**
   Specifies a unique name for the component. This option is required for the commands **create**, **delete**, and **modify**.

◆ **partition**
   Displays the administrative partition within which the component resides.
Port-transparency
Enables or disables the preservation of the destination port specified by the client over the WAN. The default value is enabled.

Regex
Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. For a description of regular expression syntax, see the regex man page.

Reuse-connection
Enables or disables the saving and reuse of connections between the local and remote WAN Optimization Managers. The default value is enabled.

Target-virtual
For terminated iSession traffic, specifies the matching criteria that a client-side BIG-IP® system uses to select a target virtual server on the server-side BIG-IP system. The default value is virtual-match-all.

The options are:

- **None**
  Specifies that the system sends the terminated iSession traffic directly to the server.

- **Host-match-all**
  Specifies that the system selects the closest match from all the host virtual servers.

- **Host-match-no-iSession**
  Specifies that the system matches only host virtual servers with no iSession profile.

- **Virtual-match-all**
  Specifies that the system selects the closest match from all the virtual servers.

See also
create, delete, glob, list, ltm virtual, modify, regex, reset-stats, show, tmsh, wom local-endpoint, wom remote-endpoint
**mapi**

Configures a Messaging Application Program Interface (MAPI) profile.

**Module**

**wom profile**

**Syntax**

Configure the `mapi` component within the `wom profile` module using the following syntax.

**Create/Modify**

- `create mapi [name]`
- `modify mapi [name]`
  - options:
    - `defaults-from [ [name] | none]`
    - `description [string]`
    - `discover-exchange-servers [disabled | enabled]`
    - `native-compression [disabled | enabled]`

**Display**

- `list mapi`
- `list mapi [ [ [name] | [glob] | [regex] ] ... ]`
- `show running-config mapi`
  - `show running-config mapi [ [ [name] | [glob] | [regex] ] ... ]`
    - options:
      - `all-properties`
      - `app-service`
      - `non-default-properties`
      - `one-line`
      - `partition`
- `show mapi`
- `show mapi [ [ [name] | [glob] | [regex] ] ... ]`
  - options:
    - `(default | exa | gig | kil | meg | peta | raw | tera | yotta | zetta)`

**Delete**

- `delete mapi [name]`
Description

You can use the `mapi` component to manage a MAPI profile.

Examples

Creates a MAPI profile named `my_mapi_profile` using the system defaults:

```
create mapi my_mapi_profile
```

Turns on `native-compression` for the MAPI profile named `my_mapi_profile`:

```
modify mapi my_mapi_profile native-compression enabled
```

Options

You can use these options with the `mapi` component:

- **app-service**
  Displays the application service to which the object belongs. The default value is `none`.
  
  *Note: If the strict-updates option is enabled on the Application Service that owns the object, you cannot modify or delete the object. Only the Application Service can modify or delete the object.*

- **defaults-from**
  Specifies the profile that you want to use as the parent profile. Your new profile inherits all settings and values from the parent profile specified. The default value is `mapi`.

- **description**
  User-defined description.

- **discover-exchange-servers**
  Enables or disables the automatic discovery of the Microsoft Exchange servers in the network and creation of a virtual server for each one discovered. The default value is `disabled`.

- **glob**
  Displays the items that match the `glob` expression. For a description of `glob` expression syntax, see the `glob` man page.

- **name**
  Specifies a unique name for the component. This option is required for the commands `create`, `delete`, and `modify`.

- **native-compression**
  Enables or disables native Microsoft Exchange compression. The default value is `disabled`.

- **partition**
  Displays the administrative partition within which the component resides.
♦ **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. For a description of regular expression syntax, see the `regex` man page.

**See also**

`create`, `delete`, `glob`, `list`, `ltm virtual`, `modify`, `regex`, `show`, `tmsh`
Glossary
address resolution protocol
Address Resolution Protocol (ARP) is an industry-standard protocol that
determines a host’s Media Access Control (MAC) address based on its IP
address.

administrative partition
An administrative partition is a logical container that you create, containing
a defined set of BIG-IP® system objects, such as virtual servers, pools, and
profiles. See also pool, profile, and virtual server.

allow list
An allow list displays which service and protocol ports allow connections
from outside the system.

ARP
See address resolution protocol.

authentication
Authentication is the process of verifying a user’s identity when the user is
attempting to log in to a system.

authentication profile
An authentication profile is a configuration tool that you use to implement a
pluggable authentication module (PAM). Types of authentication modules
that you can implement with an authentication profile are: LDAP, RADIUS,
TACACS+, SSL Client Certificate LDAP, and OCSP. See also profile.

bigdb
Every BIG-IP system includes a bigdb database. The bigdb database holds a
set of bigdb configuration keys that define the behavior of various aspects of
the BIG-IP system.

certificate
A certificate is an online credential signed by a trusted certificate authority
and used for SSL network traffic as a method of authentication. See also
certificate authority (CA).

certificate authority (CA)
A certificate authority is an external, trusted organization that issues a
signed digital certificate to a requesting computer system for use as a
credential to obtain authentication for SSL network traffic. See also
certificate.
Glossary

**Certificate revocation list**
A certificate revocation list (CRL) is a list that an authenticating system checks to see if the SSL certificate that the requesting system presents for authentication has been revoked. See also *certificate*.

**Certificate verification**
Certificate verification is the part of an SSL handshake that verifies that a client’s SSL credentials have been signed by a trusted certificate authority. See also *certificate*.

**Chunking**
Chunking refers to the HTTP 1.1 feature known as chunked encoding, which allows HTTP messages to be broken up into several parts. Chunking is most often used by servers when sending responses.

**Class**
A class is a list of data that you define and use with iRules® operators. Internal classes are stored in the `bigip.conf` file. External classes are stored in external files that you define.

**Client-side SSL profile**
A client-side SSL profile is an SSL profile that controls the behavior of SSL traffic going from a client system to the BIG-IP system. See also *profile*.

**Clone pool**
A clone pool replicates all traffic coming into it, and sends that traffic to a duplicate pool. See also *pool*.

**Configuration object**
A configuration object is a user-created object that the BIG-IP system uses to implement a PAM authentication module. There is one type of configuration object for each type of authentication module that you create.

**Configuration utility**
The Configuration utility is the browser-based application that you use to configure the BIG-IP system.

**Connection persistence**
Connection persistence is an optimization technique whereby a network connection is intentionally kept open for the purpose of reducing handshaking.

**Cookie persistence**
Cookie persistence is a mode of persistence where the BIG-IP system stores persistent connection information in a cookie.
CRL

See certificate revocation list.

current partition

When a user logs on, the system determines the default current partition (usually the partition Common) based on the user’s logon account. If the user’s account grants permission to access more than one partition, the user can change the current partition, and can also change the default current partition. See also administrative partition.

custom monitor

A custom monitor is a user-created monitor. See also monitor.

custom profile

A custom profile is a user-created profile. A custom profile can inherit its default settings from a parent profile that you specify. See also profile.

default-deny policy

A default-deny policy restricts Internet access to everything that is not explicitly permitted.

failover

Failover is the process whereby a standby unit in a redundant system takes over when a software failure or a hardware failure is detected on the active unit. See also redundant system.

floating IP address

An IP address assigned to a VLAN and shared between two computer systems is known as a floating IP address. See also VLAN (virtual local area network).

glob matching

glob matching is a pattern matching facility that the tmsh command completion feature uses to complete object identifiers.

hash persistence

Hash persistence allows you to create a persistence hash based on an existing iRule. See also iRules.

health monitor

A health monitor checks a node to see if it is up and functioning for a given service. If the node fails the check, it is marked down. Different monitors exist for checking different services. See also monitor.
host
A host is a virtual server that represents a specific site, such as an Internet web site or an FTP site, and it load balances traffic targeted to content servers that are members of a pool. See also virtual server and pool.

HTTP redirect
An HTTP redirect sends an HTTP 302 Object Found message to clients. You can configure a pool with an HTTP redirect to send clients to another node or virtual server if the members of the pool are marked down. See also virtual server and pool.

HTTP header transformation
When the BIG-IP system performs an HTTP transformation, the system manipulates the Connection header of a server-side HTTP request, to ensure that the connection stays open.

ICMP
See internet control message protocol.

interface
A physical port on a BIG-IP system is called an interface.

internal VLAN
The internal VLAN is a default VLAN on the BIG-IP system. In a basic configuration, this VLAN has the administration ports open. In a normal configuration, this is a network interface that handles connections from internal servers. See also VLAN (virtual local area network).

internet control message protocol
Internet Control Message Protocol (ICMP) is an Internet communications protocol used to determine information about routes to destination addresses.

iRules
iRules® are scripts that you write to direct and manipulate the way that the BIG-IP system manages application traffic.

last hop
A last hop is the final hop a connection takes to get to the BIG-IP system. You can allow the BIG-IP system to determine the last hop automatically to send packets back to the device from which they originated. You can also specify the last hop manually by making it a member of a last hop pool. See also pool.
Layer 1 through Layer 7

Layers 1 through 7 refer to the seven layers of the Open System Interconnection (OSI) model. Thus, Layer 2 represents the data-link layer, Layer 3 represents the IP layer, and Layer 4 represents the transport layer (TCP and UDP). Layer 7 represents the application layer, handling traffic such as HTTP and SSL.

LDAP

Lightweight Directory Access Protocol (LDAP) is an Internet protocol that email programs use to look up contact information from a server.

LDAP authentication module

An LDAP authentication module is a user-created module that you implement on an BIG-IP system to authenticate client traffic using a remote LDAP server. See also LDAP.

LDAP client certificate SSL authentication module

An LDAP client certificate SSL authentication module is a user-created module that you implement on an BIG-IP system to authorize client traffic using SSL client credentials and a remote LDAP server. See also LDAP.

link aggregation

The main objective of link aggregation is to provide increased bandwidth at a lower cost, without having to upgrade hardware. The bandwidth of the aggregated trunk is the sum of the capacity of individual member links. Thus it provides an option for linearly incremental bandwidth as opposed to bandwidth options available through physical layer technology. The traffic management system supports link aggregation control protocol (LACP).

load balancing method

A load balancing method is a method of determining how to distribute connections across a load balancing pool. See also pool.

local traffic management

Local traffic management is the process of managing network traffic that comes into or goes out of a local area network (LAN), including an intranet.

MAC

Media Access Control (MAC) is a protocol that defines the way workstations gain access to transmission media, and is most widely used in reference to LANs. For IEEE LANs, the MAC layer is the lower sublayer of the data link layer protocol.

MAC address

A MAC address is used to represent hardware devices on an Ethernet network. See also MAC.
management interface

The management interface is a special port on the BIG-IP system, used for managing administrative traffic. Named MGMT, the management interface does not forward user application traffic, such as traffic slated for load balancing.

management route

A management route is a route that forwards traffic through the special management (MGMT) interface. See also management interface.

MCPD service

The Master Control Program Daemon (MCPD) service manages the configuration data on a BIG-IP system.

MGMT

See management interface.

monitor

The BIG-IP system uses monitors to determine whether nodes are up or down. There are several different types of monitors, and they use various methods to determine the status of a server or service.

monitor association

A monitor association is an association that a user makes between a health or performance monitor and a pool, pool member, or node. See also monitor.

NAT (network address translation)

A Network Address Translation (NAT) is an alias IP address that identifies a specific node managed by the BIG-IP system to the external network.

network virtual server

A network virtual server is a virtual server whose IP address has no bits set in the host portion of the IP address (that is, the host portion of its IP address is 0). There are two kinds of network virtual servers: those that direct client traffic based on a range of destination IP addresses, and those that direct client traffic based on specific destination IP addresses that the BIG-IP system does not recognize. See also virtual server.
	node

A node is a logical object on the BIG-IP system that identifies the IP address of a physical resource on the network. Nodes are directly associated with pool members and monitors. See also pool member and monitor.
node address

A node address is the IP address associated with one or more nodes. This IP address can be the real IP address of a network server, or it can be an alias IP address on a network server.

non-terminated SSL session

A non-terminated SSL session is a session in which the system does not perform the tasks of SSL certificate authentication, encryption, and re-encryption. See also SSL (Secure Sockets Layer).

OCSP (online certificate status protocol)

Online Certificate Status Protocol (OCSP) is a protocol that authenticating systems can use to check on the revocation status of digitally-signed SSL certificates. The use of OCSP is an alternative to the use of a CRL. See also certificate revocation list.

OCSP responder

An OCSP responder is an external server used for communicating SSL certificate revocation status to an authentication server such as the BIG-IP system. See also OCSP (online certificate status protocol).

OneConnect

The F5 Networks OneConnect™ feature optimizes the use of network connections by keeping server-side connections open and pooling them for re-use.

packet rate

The packet rate is the number of data packets per second processed by a server.

PAM

A pluggable authentication module (PAM) is a mechanism that integrates multiple low-level authentication schemes into a high-level application programming interface.

partition

See administrative partition.

passive failure

A passive failure is a pool member connection failure.

persistence profile

A persistence profile is a pre-configured object that automatically enables persistence when you assign the profile to a virtual server. See also profile.
Glossary

pluggable authentication module

See PAM.

pool

A pool is composed of a group of network devices (called members). The BIG-IP system load balances requests to the nodes within a pool based on the load balancing method and persistence method you choose when you create the pool or edit its properties.

pool member

A pool member is a server that is a member of a load balancing pool. See also pool.

pre-configured monitor

A pre-configured monitor is a monitor that the BIG-IP system provides. See also monitor.

profile

A profile is a configuration tool containing settings for defining the behavior of network traffic. The BIG-IP system contains profiles for managing FastL4, HTTP, TCP, FTP, SSL, and RTSP traffic, as well as for implementing persistence and application authentication.

Quality of Service (QoS) level

The Quality of Service (QoS) level is a means by which network equipment can identify and treat traffic differently based on an identifier. Essentially, the QoS level specified in a packet enforces a throughput policy for that packet. See also type of service (ToS) level.

rate class

A rate class determines the volume of traffic allowed through a rate filter.

rate shaping

Rate shaping is a type of extended IP filter. Rate shaping uses the same IP filter method but applies a rate class, which determines the volume of network traffic allowed.

redundant system

A redundant system is a pair of units that are configured for fail-over. Of the two units, one is running as the active unit and one is running as the standby unit. If the active unit fails, the standby unit takes over and manages connection requests.

SCF (single configuration file)

An SCF is a flat, text file with an extension of .scf that contains the configuration of a BIG-IP system.
self IP address

A self IP address is an IP address that is assigned to the system. Self IP addresses are part of the base configuration. You must define at least one self IP address for each VLAN.

SIP persistence

SIP persistence is a type of persistence used for servers that receive Session Initiation Protocol (SIP) messages sent through UDP. SIP is a protocol that enables real-time messaging, voice, data, and video.

SNAT (secure network address translation)

A SNAT is a feature you can configure on the BIG-IP system. A SNAT defines a routable alias IP address that one or more nodes can use as a source IP address when making connections to hosts on the external network.

SNAT pool

A SNAT pool is a pool of translation addresses that you can map to one or more original IP addresses. Translation addresses in a SNAT pool are not self IP addresses. See also pool.

spanning tree protocol (STP)

Defined by IEEE, Spanning Tree Protocol (STP) is a protocol that provides loop resolution in configurations where one or more external switches are connected in parallel with the BIG-IP system.

SSH

SSH (secure shell) is a protocol for secure remote logon and other secure network services over a non-secure network.

SSL (Secure Sockets Layer)

Secure Sockets Layer (SSL) is a network communications protocol that uses public-key technology as a way to transmit data in a secure manner.

SSL persistence

SSL persistence is a type of persistence that tracks non-terminated SSL sessions, using the SSL session ID. See also SSL (Secure Sockets Layer).

SSL profile

An SSL profile is a configuration tool that you use to initiate and end SSL connections from clients and servers. See also SSL (Secure Sockets Layer) and profile.
TACACS

Terminal Access Controller Access Control System (TACACS) is an older authentication protocol common to UNIX® systems. TACACS allows a remote access server to forward a user’s logon password to an authentication server.

TACACS+

TACACS+ is an authentication mechanism designed as a replacement for the older TACACS protocol. There is little similarity between the two protocols, however, and they are therefore not compatible. See also TACACS.

Tcl

See Tools Command Language.

TMM service

See Traffic Management Microkernel Service.

Tools Command Language

Tools Command Language (Tcl) is an industry-standard scripting language. On the BIG-IP system, users use Tcl to write iRules. See also iRules.

topology statement

A topology statement is a set of characteristics that identify the origin of a given name resolution request.

ToS level

See type of service (ToS) level.

Traffic Management Microkernel Service

The Traffic Management Microkernel (TMM) service is the process running on the BIG-IP system that performs most traffic management for the product.

trunking

Trunking is link aggregation that allows multiple physical links to be treated as one logical link. See also link aggregation.

trusted CA file

A trusted CA file is a file containing a list of certificate authorities that an authenticating system can trust when processing client requests for authentication. A trusted CA file resides on the authenticating system and is used for authenticating SSL network traffic. See also certificate authority.
trusted MAC address

A trusted MAC address is a MAC address that passes MAC address-based authentication. See also MAC address.

type of service (ToS) level

The Type of Service (ToS) level is another means, in addition to the QoS level, by which network equipment can identify and treat traffic differently based on an identifier. See also Quality of Service (QoS) level.

UCS (user configuration set)

A UCS is an archive of all of the BIG-IP system configuration files stored in a file with an extension of .ucs.

user role

A user role is a type and level of access that you assign to a BIG-IP system user account. By assigning user roles, you can control the extent to which BIG-IP system administrators can view or modify the BIG-IP system configuration.

vCMP

Virtualized Clustered Multiprocessing (vCMP) is a feature of the BIG-IP system that allows you to run multiple instances of the BIG-IP software on a single F5 Networks hardware platform.

virtual address

A virtual address is an IP address associated with one or more virtual servers managed by the BIG-IP system.

virtual server

A virtual server is a specific combination of virtual address and virtual port, associated with a content site that is managed by an BIG-IP system or other type of host server.

VLAN (virtual local area network)

A VLAN is a logical grouping of interfaces connected to network devices. You can use a VLAN to logically group devices that are on different network segments. Devices within a VLAN use Layer 2 networking to communicate and define a broadcast domain.

VLAN group

A VLAN group is a logical container that includes two or more distinct VLANs. VLAN groups are intended for load balancing traffic in a Layer 2 network, when you want to minimize the reconfiguration of hosts on that network. See also VLAN (virtual local area network).
Index
A
aaa-active-directory component 9-2
aaa-client-cert component 9-6
aaa-crldp component 9-8
aaa-http component 9-10
aaa-ldap component 9-12
aaa-oocsp component 9-15
aaa-radius component 9-17
aaa-securid component 9-19
access component 10-2
access-policy component 8-2
acct-radius component 9-21
acct-tacacsp plus component 9-23
acl component 5-2
active-directory component 6-2
admin-partitions component 16-2
advertised-route component 52-2
all-stats component 46-2
analytics component 33-2
analytics module 4-1
apache-ssl-cert component 45-2
apls-script component 40-2
apm aaa module 6-1
apm epsec module 7-1
apm module 5-1
apm policy agent module 9-1
apm policy module 8-1
apm profile module 10-1
apm resource module 11-1
apm resource remote-desktop module 12-1
apm sso module 13-1
application component 51-2
application-volume component 44-2
app-tunnel component 11-2
arp component 35-2
array component 47-2
asm module 14-1
audit entries table 2-15
audit file 2-14
audit log 2-14
auth module 15-1

B
base configuration, saving and loading 2-2
basic component 13-2
batch mode 2-22
bay component 47-4
bigip component 21-2
bigip-link component 21-6
bigstart command 1-2
bigtop utility, defined 1-2
by-handle component 42-2

C
category component 24-2
cd command 3-2
cert component
  for cm module 18-2
  for crypto module 41-2
certificate-authority component 33-11
cert-ldap component 15-2
check-cert component 41-5
cifs component 53-2
citrix component 12-2
citrix-client-bundle component 12-6
citrix-client-package-file component 12-8
class component 37-2
classification component 33-14
cli alias module 17-1
cli module 16-1
client-rate-class component 11-5
client-ssl component 33-16
client-traffic-classifier component 11-9
clock component 39-2
cluster component 39-3
clusterd component 43-2
cm module 18-1
cmetrics component 35-5
command alias 2-16
command audit 2-14
command completion feature 2-7
command history feature 2-10
command line utilities 1-2
command syntax
  global commands 3-1
commands
  about global 3-1
  See specific command name.
component mode, leaving 2-6
component, global 3-46
components
  navigating out of 2-6
  navigating to 2-1
  working within 2-4
  See individual component name.
config component 39-6
config utility
  using to set up the BIG-IP system 1-2
config-diff component 39-12
config-sync component 18-6
connection component
  for ltm global-settings module 30-2
  for sys module 39-13
connections component 46-4
connectivity component 10-8
console component 39-16
context-sensitive help 2-9
cookie component 32-2
cp command 3-4
cpu component 39-18
create command 3-6
crl component 41-7
crdp component 6-5
crdp-server component 23-2
csyncd component 43-4
customization-group component 8-3
custom-stat component 40-4

d
daemon-ha component 39-19
datacenter component 19-2
data-group component 45-5
datastor component 39-22
db component
  for ltm dns dns-express module 28-2
  for sys module 39-24
decision-box component 9-25
deduplication component 52-5
default-config component 39-27
default-node-monitor component 22-2
delete command 3-8
dest-addr component 32-6
device component 18-8
device-group component 18-12
device-sync component 14-2
diagnose-conn component 52-7
diameter component
  for ltm monitor module 31-2
  for ltm profile module 33-24
disk component 47-6
distributed-app component 19-5
dns component
  for ltm monitor module 31-7
  for ltm profile module 33-28
  for sys module 39-28
drop-policy component 37-7
dynamic-acl component 9-27

E
edit command 3-10
ending-allow component 9-29
ending-deny component 9-31
ending-redirect component 9-33
endpoint-check-av component 9-35
endpoint-check-fw component 9-38
endpoint-discovery component 52-8
endpoint-linux-check-file component 9-41
endpoint-linux-check-process component 9-44
endpoint-mac-check-file component 9-46
endpoint-mac-check-process component 9-49
endpoint-windows-browser-cache-cleaner component 9-51
endpoint-windows-check-file component 9-54
endpoint-windows-check-machine-cert component 9-58
endpoint-windows-check-process component 9-61
endpoint-windows-check-registry component 9-63
endpoint-windows-group-policy component 9-66
endpoint-windows-info-os component 9-68
endpoint-windows-machine-info component 9-70
endpoint-windows-protected-workspace component 9-72
epsec-package component 7-2
etherip component 38-2
exit command 3-13
external component
  for gtm monitor module 21-9
  for ltm data-group module 25-2
  for ltm monitor module 31-12
external-logon-page component 9-74
external-monitor component 45-8

F
failover component 39-30
failover-status component 18-15
fasthttp component 33-31
fastl4 component 33-36
fdb component 35-7
firepass component
  for gtm monitor module 21-13
  for ltm monitor module 31-16
folder component 39-33
form-based component 13-5
form-basedv2 component 13-9
ftp component
  for gtm monitor module 21-17
  for ltm monitor module 31-20
  for ltm profile module 33-41

g
gateway-icmp component
  for gtm monitor module 21-21
  for ltm monitor module 31-24
gencert utility, defined 1-2
general component
  for gtm global-settings module 20-2
  for ltm global-settings module 30-4
generate command 3-14
generation components 29-2
geloip component 39-36
glob 2-7
glob matching 2-7
global component 3-46
  for vcmp module 50-2
global-settings component 16-3
  for cli module 16-3
  for ltm dns cache module 26-2
  for ltm persistence module 32-9
  for sys module 39-37
gre component 38-5
grep 2-21

gtm component 46-6

tgm global-settings module 20-1

tgm module 19-1

tgm monitor module 21-1

tgm pool component 19-23

guest component 50-3

H

ha-group component 39-42

hardware component 39-45

hash component 32-11

ha-status component 39-46

help

   using context-sensitive 2-9

help command 3-15

historical logs 2-16

history 2-10

history component 16-6

history feature, for commands 2-10

host-info component 39-47

hotfix component 48-2

http component

   for apm aaa module 6-8
   for apm module 6-8
   for gtm monitor module 21-25
   for ltm monitor module 31-28
   for ltm profile module 33-44

httpclass component 33-50

http-class-asm component 14-3

http-compression component 33-54

httpd component 39-48

https component

   for gtm monitor module 21-29
   for ltm monitor module 31-33

http-signature component 24-4

hypervisor-info component 39-52

I

icmp component 31-38

icmp-stat component 39-53

ifile component 22-4

iiop component 33-59

ike-daemon component 36-2

ike-peer component 36-4

image component 48-5

image-file component 8-4

imap component

   for gtm monitor module 21-34
   for ltm monitor module 31-42

inband component 31-46

install command 3-17

interface component 35-10

internal component 25-6

ip-address component 39-54

ipip component 38-8

iprep-status component 39-56

ipsec-policy component 36-9

ip-stat component 39-58

ipv6-leasepool component 11-12

iqqery component 39-58

irule-event component 9-76

isession component 53-5

K

kerberos component 6-11

   for apm aaa module 6-11
   for apm policy agent module 9-79
   for apm sso module 13-18

kerberos-delegation component 23-5

kerberos-keytab-file component 6-13

key

   for ltm classification module 24-7

   for cm module 18-16
   for ltm dns cache records module 27-2
   for ltm dns dnssec module 29-4
   for sys crypto module 41-9

keyboard map feature

   and default settings 2-13
   using 2-13

L

ldap component

   for apm aaa module 6-15
   for apm module 6-15
   for auth module 15-8
   for gtm monitor module 21-38
   for ltm auth module 23-8
   for ltm monitor module 31-49

ldns component 19-10

leasepool component 11-14

license component 39-59

lind component 43-6

link component 19-11

list command 3-18

listener component 19-16

load command 3-21

load-balancing component 20-6

loading the system configuration 2-2

local-endpoint component 52-11

log component 39-60

log entries

   for audit 2-15
   for history 2-16

logging component 9-81

logical-disk component 44-4

login-failures command 15-13

logon-page component 9-83

log-rotate component 39-62
Index

ltm auth module 23-1
ltm classification module 24-1
ltm data-group module 25-1
ltm dns cache module 26-1
ltm dns cache records module 27-1
ltm dns dns express module components 28-1
ltm dns nssec module 29-1
ltm module 22-1
ltm pool component 22-13
ltm tce module 34-1

M
mac-address component 39-65
man pages 2-8
management-ip component 39-67
management-route component 39-69
manual-security-association component 36-12
mapi component 53-9
master-key component 41-13
mblb component 33-62
mcpd component 43-8
mcp-state component 39-72
memory component 39-73
message-box component 9-87
metrics component 20-8
metrics-exclusions component 20-11
modify command 3-22
module
  leaving 2-6
  navigating to 2-3
  working within 2-3
module-score component 31-54
msg component 27-4
msrdp component 32-15
mysql component
  for gtm monitor module 21-43
  for ltm monitor module 31-58
mv component 3-24
mysql component
  for gtm monitor module 21-48
  for ltm monitor module 31-63

N
nameserver component 27-6
nat component 22-6
ndp component 35-15
net ipsec module 36-1
net tunnels module 38-1
network-access component 11-16
nttp component
  for gtm monitor module 21-53
  for ltm monitor module 31-68
node component 22-9
normalization component 51-7
ntlm component 33-65
ntlmv1 component 13-22
ntlmv2 component 13-25
ntp component 39-74

O
oam component 9-89
  for apm aaa module 6-18
  for apm policy agent module 6-18
object mode
  leaving 2-6
  working in 2-5
object-type component 51-10
ocsp component 6-22
ocsp-responder component 23-13
oneconnect component 33-68
Openssl utility 1-2
oracle component
  for gtm monitor module 21-57
  for ltm monitor module 31-72

P
packet-filter component 35-17
packet-filter-trusted component 35-22
partition component 15-15
password component 15-17
password-policy component 15-18
path component 19-20
persist component 19-21
persist-records component 32-18
pkcs12 component 41-15
policy 8-5
policy component
  for ltm tce module 34-2
  for wam module 51-13
policy-item component 8-5
pool component 22-13
  for gtm module 19-23
  for ltm module 22-13
pop3 component
  for gtm monitor module 21-62
  for ltm monitor module 31-77
portal-access component 11-24
port-mirror component 35-25
postgresql component
  for gtm monitor module 21-66
  for ltm monitor module 31-81
ppp component 38-11
predefined-policy component 14-5
preference component 16-8
preferences
  for show-aliases 2-17
  for statistics 2-18
private component 17-2
private-key component 42-3
prober-pool component 19-35

Index - 4
<table>
<thead>
<tr>
<th>Index</th>
</tr>
</thead>
<tbody>
<tr>
<td>proc-info component</td>
</tr>
<tr>
<td>profile component</td>
</tr>
<tr>
<td>provision component</td>
</tr>
<tr>
<td>public-key component</td>
</tr>
<tr>
<td>publish command</td>
</tr>
<tr>
<td>pva-traffic component</td>
</tr>
<tr>
<td>pwd component</td>
</tr>
<tr>
<td>Q</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>R</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>S</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>
Index

smtp-dca-base component 31-126
smtp-link component 21-99
soap component
  for gtm monitor module 21-103
  for ltm monitor module 31-129
software-status component 7-4
source component 15-34
source-addr component 32-24
spdy component 33-101
special characters 2-24
sshd component 39-105
ss component 32-28
ssl-cc-ldap component 23-28
ssl-cert component 45-11
ssl-crl component 45-14
ssl-crldp component 23-33
ssl-key component 45-16
ssl-oscp component 23-36
start command 3-43
state-mirroring component 39-109
statistics component 33-104
statistics feature
  resetting 2-21
  using 2-18
statistics, viewing 2-18
status component 48-8
steering-endpoint component 34-5
stop command 3-44
stored configuration files 2-2
stp component 35-43
stp-globals component 35-47
stream component 33-108
submit command 3-45
sync-status component 18-21
syntax conventions 1-3
sys application module 40-1
sys crypto fips module 42-1
sys daemon-log-settings module 43-1
sys disk module 44-1
sys file module 45-1
sys module 39-1
sys software module 48-1
syslog component 39-113
system component 46-12
system configuration, loading and saving 2-2
T
tacacs component
  for apm aaa module 6-33
  for auth module 15-36
  for ltm auth module 23-39
tacacsplus component 9-97
tc component 33-111
tc-policy component 22-38, 34-2
Tcl, defined 1-2
tcp component
  for gtm monitor module 21-108
  for ltm monitor module 31-134
  for ltm profile module 33-113
tcp-echo component 31-139
tcp-half-open component
  for gtm monitor module 21-112
  for ltm monitor module 31-143
template component 40-9
test-monitor component 49-2
throughput component 46-14
tm profile module 33-1
tmm component 43-10
tmm-info component 39-117
tmm-traffic component 39-118
TMOS 1-1
tmsh
  and command completion 2-7
  and command history 2-10
  and command syntax 2-2
  and modular structure 2-1
  closing 2-6
  introducing 1-1
  tmsh hierarchy
    understanding 2-1
    working within 2-3
tmsh modules, working with 2-1
tmsh prompt 2-2
Tools Command Language 1-2
topology component 19-52
tracepath component 49-3
tracepath6 component 49-4
traceroute component 49-5
traceroute6 component 49-6
traffic component
  for gtm module 19-55
  for system module 39-119
Traffic Management Operating System 1-1
Traffic Management Shell
  See tmsh.
  traffic-class component 22-41
  traffic-control component 30-6
  traffic-group component 18-22
  traffic-selector component 36-15
transaction component 16-31
transparent component 26-8
trunk component 35-51
trust-domain component 18-25
tsig-key component 28-3
tunnel component 38-14
U
ucs component 39-120
udp component
  for gtm monitor module 21-116
for ltm monitor module 31-147
for ltm profile module 33-120
universal component 32-31
update-signatures component 24-11
user component 15-40

V
validating-resolver component 26-11
variable-assign component 9-99
vconsole component 49-7
vdisk component 50-7
verify-config component 52-23
version component 39-122
virtual component 22-44
virtual-address component 22-52
virtual-location component 31-152
vlan component 35-56
vlan-allowed component 35-60
vlan-group component 35-61
volume component 48-10

W
wa-cache component 33-123
wam module 51-1
wap component
  for gtm monitor module 21-120
  for ltm monitor module 31-156
watch-devicegroup-device component 18-29
watch-sys-device component 18-31
watch-trafficgroup-device component 18-33
wccp component
  for net module 35-65
  for net tunnels 38-17
webapp-language component 14-7
webtop component 11-28
webtop-link component 11-31
wideip component 19-56
wildcard search 2-18
windows-group-policy-file component 8-6
wmi component
  for gtm monitor module 21-125
  for ltm monitor module 31-161
wom module 52-1
wom profile module 53-1

X
xml component 33-125

Z
zebos component 49-8
zone component
  for ltm dns dns-express module 28-5
  for ltm dns dnssec module 29-8