Enterprise Manager™: Monitoring Network Health and Activity

Version 3.1.1

Table of Contents

Legal Notices

Publication Date

This document was published on March 20, 2015.

Publication Number

MAN-0396-02

Copyright

Trademarks

AAM, Access Policy Manager, Advanced Client Authentication, Advanced Firewall Manager, Advanced Routing, AFM, Alive With F5, APM, Application Acceleration Manager, Application Security Manager, ARX, AskF5, ASM, BIG-IP, BIG-IQ, Cloud Extender, CloudFucious, Cloud Manager, Clustered Multiprocessing, CMP, COHESION, Data Manager, DevCentral, DevCentral [DESIGN], DNS Express, DSC, DSI, Edge Client, Edge Gateway, Edge Portal, ELEVATE, EM, Enterprise Manager, ENGAGE, F5, F5 [DESIGN], F5 Certified [DESIGN], F5 Networks, Fast Application Proxy, Fast Cache, FirePass, Global Traffic Manager, GTM, GUARDIAN, iApps, IBR, Intelligent Browser Referencing, Intelligent Compression, IPv6 Gateway, iControl, iHealth, iQuery, iRules, iRules OnDemand, iSession, L7 Rate Shaping, LC, Link Controller, Local Traffic Manager, LTM, LineRate, LineRate Systems [DESIGN], LROS, Message Security Manager, MSM, OneConnect, Packet Velocity, PEM, Policy Enforcement Manager, Protocol Security Manager, PSM, Real Traffic Policy Builder, Scale^{N}, Signalling Delivery Controller, SDC, SSL Acceleration, StrongBox, SuperVIP, SYN Check, TCP Express, TDR, TMOS, Traffic Management Operating System, Traffix Systems, Traffix Systems (DESIGN), Transparent Data Reduction, UNITY, VAULT, VIPRION, vCMP, VE F5 [DESIGN], Virtual Clustered Multiprocessing, WA, WAN Optimization Manager, WebAccelerator, WOM, and ZoneRunner, are trademarks or service marks of F5 Networks, Inc., in the U.S. and other countries, and may not be used without F5's express written consent.

All other product and company names herein may be trademarks of their respective owners.

Patents

This product may be protected by one or more patents indicated at:
http://www.f5.com/about/guidelines-policies/patents

Export Regulation Notice

This product may include cryptographic software. Under the Export Administration Act, the United States government may consider it a criminal offense to export this product from the United States.

RF Interference Warning

This is a Class A product. In a domestic environment this product may cause radio interference, in which case the user may be required to take adequate measures.

FCC Compliance

This equipment has been tested and found to comply with the limits for a Class A digital device pursuant to Part 15 of FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This unit generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, 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 ICES-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 Bill Paul.

This product includes software developed by Jonathan Stone.

This product includes software developed by Manuel Bouyer.

This product includes software developed by Paul Richards.

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

This product includes software developed by the Politecnico di Torino, and its contributors.

This product includes software developed by the Swedish Institute of Computer Science and its contributors.

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 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 the University of Vermont and State Agricultural College and Garrett A. Wollman.

This product includes software developed by Balazs Scheidler (bazsi@balabit.hu), which is protected under the GNU Public License.

This product includes software developed by Niels Mueller (nisse@lysator.liu.se), which is protected under the GNU Public License.

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).

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 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.

This product includes software developed by Jared Minch.

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/).

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com).

This product contains software based on oprofile, which is protected under the GNU Public License.

This product includes RRDtool software developed by Tobi Oetiker (http://www.rrdtool.com/index.html) and licensed under the GNU General Public License.

This product contains software licensed from Dr. Brian Gladman under the GNU General Public License (GPL).

This product includes software developed by the Apache Software Foundation (http://www.apache.org/).

This product includes Hypersonic SQL.

This product contains software developed by the Regents of the University of California, Sun Microsystems, Inc., Scriptics Corporation, and others.

This product includes software developed by the Internet Software Consortium.

This product includes software developed by Nominum, Inc. (http://www.nominum.com).

This product contains software developed by Broadcom Corporation, which is protected under the GNU Public License.

This product contains software developed by MaxMind LLC, and is protected under the GNU Lesser General Public License, as published by the Free Software Foundation.

This product includes Intel QuickAssist kernel module, library, and headers software licensed under the GNU General Public License (GPL).

This product includes software developed by members of the CentOS Project under the GNU Public License, copyright ©2004-2011 by the CentOS Project.

This product includes software developed by members of the OpenJDK Project under the GNU Public License Version 2, copyright ©2012 by Oracle Corporation.

This product includes software developed by The VMWare Guest Components Team under the GNU Public License Version 2, copyright ©1999-2011 by VMWare, Inc.

This product includes software developed by The Netty Project under the Apache Public License Version 2, copyright ©2008-2012 by The Netty Project.

This product includes software developed by Stephen Colebourne under the Apache Public License Version 2, copyright ©2001-2011 Joda.org.

This product includes software developed by the GlassFish Community under the GNU Public License Version 2 with classpath exception, copyright ©2012 Oracle Corporation.

This product includes software developed by the Mort Bay Consulting under the Apache Public License Version 2, copyright ©1995-2012 Mort Bay Consulting.

This product contains software developed by members of the Jackson Project under the GNU Lesser General Public License Version 2.1, ©2007 – 2012 by the Jackson Project".

This product contains software developed by QOS.ch under the MIT License, ©2004 – 2011 by QOS.ch.

This product includes software licensed from Gerald Combs (gerald@wireshark.org) under the GNU General Public License as published by the Free Software Foundation; either version 2 of the License, or any later version. Copyright ©1998 Gerald Combs.

This product includes software developed by Thomas Williams and Colin Kelley. Copyright ©1986 - 1993, 1998, 2004, 2007

Permission to use, copy, and distribute this software and its documentation for any purpose with or without fee is hereby granted, provided that the above copyright notice appear in all copies and that both that copyright notice and this permission notice appear in supporting documentation. Permission to modify the software is granted, but not the right to distribute the complete modified source code. Modifications are to be distributed as patches to the released version. Permission to distribute binaries produced by compiling modified sources is granted, provided you

1. distribute the corresponding source modifications from the released version in the form of a patch file along with the binaries,
2. add special version identification to distinguish your version in addition to the base release version number,
3. provide your name and address as the primary contact for the support of your modified version, and
4. retain our contact information in regard to use of the base software.

Permission to distribute the released version of the source code along with corresponding source modifications in the form of a patch file is granted with same provisions 2 through 4 for binary distributions. This software is provided "as is" without express or implied warranty to the extent permitted by applicable law.

This product contains software developed by Google, Inc. Copyright ©2011 Google, Inc.

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

This software incorporates JFreeChart, ©2000-2007 by Object Refinery Limited and Contributors, which is protected under the GNU Lesser General Public License (LGPL).

This product contains software developed by the Mojarra project. Source code for the Mojarra software may be obtained at https://javaserverfaces.dev.java.net/.

Chapter 1

Using iHealth for Configuration Collection and Diagnostics

Overview: iHealth

You can use BIG-IP® iHealth® to verify that the hardware and software for your managed devices is operating properly and at peak efficiency. iHealth is a tool that collects data about elements of device configuration, logs, command output, password security, license compliance, and so on. You can use the iHealth diagnostics to identify any issues that require your attention.

When you create a task to gather iHealth diagnostics, Enterprise Manager™ captures a snapshot of the specified device in the form of a qkview file. The iHealth service compares the device's information to an F5® database containing known issues, common configuration errors, and F5 published best practices. Enterprise Manager then displays the results of this evaluation, which includes:

- Descriptions of configuration issues or code defects
- Recommended solutions
- Associated link(s) to the AskF5™ Knowledge Base for reference

In many cases, you can use this customized diagnostic information to resolve common configuration issues without contacting F5 Technical Support for help. If you do require assistance from F5 Technical Support, this iHealth data can help F5 engineers provide you with a resolution more quickly.

Specifying credentials to access iHealth diagnostics service

To send iHealth® data for diagnosis, you must have an AskF5™ Knowledge Base user name and password, which you can obtain at `https://login.f5.com/resource/registerEmail.jsp`.

Use the following procedure to specify the credentials required to send collected data to the iHealth diagnostics service.

1. On the Main tab, click **Enterprise Management** > **Options** > **Devices** > **Diagnostics**.
2. In the **User Name** field type the name of the registered AskF5 Knowledge Base user.
3. In the **Password** field type the password for the registered AskF5 Knowledge Base user.
4. Click **Test Connection** to verify the credentials and connectivity to the iHealth diagnostics service.
5. Click **Save Changes**.

Enterprise Manager™ uses the credentials you specified when contacting the iHealth diagnostics service.

Gathering configuration data for diagnostics with iHealth

BIG-IP® iHealth is only available starting in Enterprise Manager™ version 2.0 and BIG-IP version 10.0.1.

You collect iHealth diagnostics data to help you verify that your devices are running efficiently, find out about upcoming events for which an action is required, and to help you troubleshoot issues.

1. On the Main tab, click **Enterprise Management** > **Tasks**.
2. For the **Support** setting, select **Gather iHealth Diagnostics**.
3. Click **Next**.
4. From the **Device List**, you can select a group of devices to narrow the number of devices displayed.
5. In the **User Name** and **Password** fields, type the registered F5 Technical Support user name and password.
6. For the **Device Filter** setting, you can select an option to display devices with a specific status.

The **Compatible Devices in Standby or Offline Mode** table refreshes to display devices that meet the criteria of the option you selected.

7. Select the check box next to the devices for which you want to gather configuration data.
8. Click the **Next** button.
   The Task Options screen opens.
9. From the **Device Error Behavior** list, select the action you want Enterprise Manager to take in the event that the task fails on one of the devices.
   - **Continue task on remaining devices**
   - **Cancel task on remaining devices**
10. Click **Next**.
    The Task Summary screen opens.
11. Click the **Start Task** button.
    The Task Properties page displays the progress for the task.

When the task completes, the Task Properties screen displays the **Progress** as `Finished`.

Creating an iHealth data collection schedule

Scheduling Enterprise Manager™ to perform a weekly data collection of iHealth diagnostics data ensures that your managed devices are working at peak efficiency and you are apprised of any upcoming system events.

1. On the Main tab, click **Enterprise Management** > **Tasks** > **Schedules**.
2. From the menu bar, click **Schedules** > **iHealth Diagnostics**.
3. From the **Collect Diagnostics Data** list, select **Weekly**.
4. From the **Day of the Week** and **Start Time** lists, select the day and time that you want Enterprise Manager to collect iHealth diagnostics data.
5. Click **Save Changes**.

On the day and time specified, Enterprise Manager collects iHealth diagnostics data.

You can view iHealth diagnostics results on the iHealth Diagnostics screen.

Viewing iHealth diagnostics

iHealth® diagnostics provides you with a snapshot of the health for the managed objects in your network and access to details about reported issues.

1. On the Main tab, click **Enterprise Management** > **Devices** > **iHealth Diagnostics**.
   The iHealth Diagnostics screen opens.
2. From the **Show** list, select an option to view devices specific to a severity level.
   The screen displays only the devices that match the severity level that you chose.
3. To view the diagnostic details specific to a device, click the name of the device.
   The iHealth Diagnostics screen opens to display the specific details about the noted issues.

Chapter 2

Using Alerts

Overview: Alerts

You can better manage the health of your network by configuring Enterprise Manager™ to alert you when specific system events occur. You can apply these alerts to individual devices, or to a device list, as well as to the Enterprise Manager device itself, so that you can monitor the events for your management system.

You can configure Enterprise Manager to manage alerts in these ways:

- Send SNMP traps to a remote SNMP server
- Send email alerts to a specific recipient using SMTP

Attention: *To perform the specific tasks required to manage alerts, you must have administrator privileges with root access for the Configuration utility.*

About configuring an SMTP server to send alert email

If you want to have a specific recipient receive an email message when an alert is triggered, you must configure Enterprise Manager™ to deliver locally-generated email messages using the internet-standard for electronic mail transmission, *Simple Mail Transfer Protocol* (*SMTP*). Before configuring SMTP email notification alerts, you must configure DNS resolution and create an SMTP server configuration.

Specifying the IP address of your DNS server

You must specify the IP address of your DNS server for communication to the F5® file servers and for SMTP email notification.

1. On the Main tab, click **System** > **Configuration** > **Device** > **DNS**.
   The DNS Device configuration screen opens.
2. In the DNS Lookup Server List area, in the **Address** field, type the IP address of the DNS server(s) you want to add.

   The system uses these DNS servers to validate DNS lookups and resolve host names. Then, click **Add**.

   Note: *If you did not disable DHCP before the first boot of the system, and if the DHCP server provides the information about your local DNS servers, then this field is automatically populated.*
3. Click **Update** to save the changes.

Verifying DNS resolution

After you specify the IP address of your DNS server, you can verify that the address properly resolves.

1. Log in to the command line as `root`.
2. Type the `dig <domain>` command.
   For example, to query `MX` and `siterequest.com`, you would type `dig siterequest.com mx`.
   The result to this query should appear similar to this example, indicating that the address properly resolves.

```
; << >> DiG 9.2.2 << >> siterequest.com mx
                ;; global options:  printcmd
                ;; Got answer:
                ;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 16174
                ;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0
                ;; QUESTION SECTION:
                ;siterequest.com.                       IN      MX
;; ANSWER SECTION:
siterequest.com.             86400   IN      MX      10 mail.siterequest.com.
;; Query time: 65 msec
;; SERVER: 172.16.100.1#53(172.16.100.1)
;; WHEN: Mon Nov  8 14:32:07 2011
;; MSG SIZE  rcvd: 51
```

Creating an SMTP server configuration

You specify the SMTP server configuration so that you can send emails through an SMTP server.

1. On the Main tab, click **System** > **Configuration** > **Device** > **SMTP**.
2. Click the **Create** button.
   The New SMTP Configuration screen opens.
3. In the **Name** field, type a name for the SMTP server that you are creating.
4. In the **SMTP Server Host Name** field, type the fully qualified domain name for the SMTP server host.
5. In the **SMTP Server Port Number** field, type a port number.
   For no encryption or TLS encryption, the default is `25`. For SSL encryption, the default is `465`.
6. In the **Local Host Name** field, type the host name used in the SMTP headers in the form of a fully qualified domain name.
   This host name is not the same as the BIG-IP system's host name.
7. In the **From Address** field, type the email address that you want displayed as the reply-to address for the email.
8. From the **Encrypted Connection** list, select the encryption level required for the SMTP server.
9. To require that the SMTP server validates users before allowing them to send email, select the **Use Authentication** check box, and type the user name and password required to validate the user.
10. Click the **Finish** button.

You can now configure the system to use this SMTP server to send emails.

Configuring SMTP email notification for alerts

To configure Enterprise Manager™ to deliver locally generated email messages (such as alerts), you must have root access privileges to its command line, the system must be configured for DNS resolution, and you must first create an SMTP server configuration.

You specify an SMTP server to send alerts to a configured email recipient.

Note: *Prior to Enterprise Manager version 3.0 and BIG-IP systems version 11.0, you configured postfix to deliver locally-generated email messages.*

---

1. On the Main tab, click **Enterprise Management** > **Options** > **Servers**.
2. In the **SMTP Server** area, from the **SMTP Configuration Name** list, select the configuration you set up for your SMTP server.
3. Click the **Save Changes** button.

Specifying defaults for alert options

Setting the default behavior for alerts ensures consistent alert actions and the ability to quickly add new alerts based on these standardized options. It is important to specify default behavior for alerts before you enable the alert options.

1. On the Main tab, click **Enterprise Management** > **Options** > **Alerts**.
2. If you want Enterprise Manager to send emails when an alert is triggered, in the **Email Recipient** field, type the email address of the user, or the alias, that you want as the default receiver for alerts.
3. If you want to log alert events to a `syslog` file:
   a) In the **Remote Syslog Server Address** field, type the IP address of the remote syslog server where you want to store alert event logs by default.
   b) In the **Maximum History Entries** field, type the maximum number of alerts that you want stored in the `syslog` file.

      If the alert history reaches the limit you set, Enterprise Manager deletes the oldest entries to create room for newer entries.

4. Click **Save Changes**.

Creating an alert for attack signature updates

Before Enterprise Manager can send alerts, you must verify the IP address of your DNS server. If you want Enterprise Manager to send SNMP traps, you must first specify the trap destination.

Create alerts for your devices to monitor specific system events.

1. On the Main tab, click **Enterprise Management** > **Alerts** > **Device Alert List**.
2. Click the **Create** button.
   The New Alert screen opens.
3. In the **Name** field, type a name for the alert.

   Once you create the alert, you cannot change the name.

4. From the **Alert Type** list, select the type of alert that you want to create.
   Depending on the type of alert that you select, the screen may refresh to display additional options, including threshold fields.
5. If the alert type requires a threshold, for the **Condition** setting, specify a threshold value.
6. For the **Action** setting, select the check box next to each action that you want Enterprise Manager to take when the alert is triggered.

   If you select the option, **SNMP trap to remote server**, you must have SNMP configured.

7. If you selected the option to send an email for this alert and you want to specify an address different than the default, clear the **Use default email recipient** check box, and in the **Email Recipient** field, type an email address.

   By default, the system sends an email to the recipient you specified in the Options screen for alerts.

8. If you selected the option to send a message to a remote syslog server and you want to specify an address different than the default, clear the **Use default remote syslog server address** check box and in the **Remote Syslog Server Address** field, type a remote syslog server address.

   By default, the system sends the event to the remote syslog server address you specified in the Options screen for alerts.

9. For the **Devices** or **Devices Lists** setting, in the **Available** box, select one or more devices from the devices or device list and click the Move button to move the selected devices or device list to **Assigned**.
10. Click **Finished**.

Enterprise Manager notifies you if a device meets the criteria for the alert you selected.

Creating an alert for Enterprise Manager

To help maintain the health of the Enterprise Manager™ device, you can create system alerts to notify you when CPU, disk, or memory usage meets or exceeds a particular threshold.

1. On the Main tab, click **Enterprise Management** > **Alerts** > **EM Alerts**.
2. For the **Conditions** setting, select the check box next to each of the metrics on which you want to set an alert.
   The screen refreshes to display threshold fields for the conditions you selected.
3. Retain the default values or type a new maximum in the threshold fields.
4. In the EM Alert Actions area, for the **Action** setting, select the type of action that you want Enterprise Manager to take when the values you specified for the thresholds are met or exceeded.
5. Click **Save Changes**.

Enterprise Manager informs you if the metrics you selected meet the thresholds you defined.

Chapter 3

Managing Traffic and System Certificates

Overview: Certificate monitoring

When you use BIG-IP® Local Traffic Manager™ to manage your SSL traffic, you must track both traffic and system certificates for the devices in your network. *Traffic certificates* are server certificates that a device uses for traffic management tasks. *System certificates* are the web certificates that allow client systems to log into the BIG-IP Configuration utility.

To assist you in overseeing these certificates, Enterprise Manager™ provides a summary of vital certificate information for each managed device in your network. The information that displays on the certificate list screen provides a summary of:

- Certificate expiration status
- Certificate and organization name
- Device on which the certificate is configured

When you monitor a device list, you automatically monitor all of the certificates on all of the devices that are members of that device list. By default, certificate monitoring is enabled for all managed devices.

Tip: *If you require additional notification about certificate expiration details, you can create a certificate expiration alert.*

Viewing certificates for a managed device

Use this procedure to view the device certificate screen.

1. On the Main tab, click **Enterprise Management** > **Devices** > **Device List**.
2. Click the name of the device for which you want to view certificate details.
   The Device Properties screen for that device opens.
3. On the Menu bar, from the **Configurations** menu, select **Monitored Certificates**.
   The Monitored Certificates screen for the selected certificate opens.
4. To view additional details about a particular certificate, click the name of the certificate.

Certificate expiration status flag definitions

The certificate list screen also displays a status flag for each certificate, to provide a quick visual indicator of the status for your certificates.

Color of status flag	Expiration status	Suggested action
Red	This certificate has expired. When client systems require this certificate for authentication, the client receives an expired certificate warning.	You must renew this certificate for proper authentication with clients.
Yellow	This certificate will expire in 30 days or less.	Although this certificate is valid, you should take action to prevent certificate expiration.
Green	This certificate is valid and will remain valid for 30 days.	No action is required.

Creating a certificate expiration alert for a device

Before you can create a certificate expiration alert, you must have certificate monitoring is enabled.

You can create an alert to log or send an email notification of an upcoming certificate expiration.

1. On the Main tab, click **Enterprise Management** > **Alerts** > **Device Alert List**.
2. Click the **Create** button.
   The New Alert screen opens.
3. In the **Name** field, type a name for the alert.

   Once you create the alert, you cannot change the name.
4. From the **Alert Type** list, select **Certificate Expiration**.
5. For the **Condition** setting, select the check box next to the number of days before the certificate expires that you want to be notified. Or, type a customized value in the **Days** field.

   Select as many options as you like to be notified multiple times about an upcoming certificate expiration.
6. For the **Action** setting, select the check box next to each action that you want Enterprise Manager to take when the alert is triggered.

   If you select the option, **Send SNMP trap to remote server**, you must have SNMP configured.
7. If you want to change the email recipient for this alert, clear the **Use default email recipient** check box and in the **Email Recipient** field, type an email address.

   The default email recipient is specified in the Options screen for alerts.
8. If you want to change the syslog server address for this alert, clear the **Use default syslog server address** check box, and in the **Syslog Server Address** field, type a syslog server address.

   The default syslog server address is specified in the Options screen for alerts.
9. For the **Devices** or **Devices Lists** setting, in the **Available** box, select one or more devices from the devices or device list and click the Move button to move the selected devices or device list to **Assigned**.
10. Click **Finished**.

Enterprise Manager informs in you in advance (according to the number of days you specified) of any upcoming certificate expiration.

Chapter 4

Logging and Auditing

Overview: Logging for devices and Enterprise Manager

Enterprise Manager™creates separate audit and system event logs specific to:

- Enterprise Manager activities associated with device management events
- System events for Enterprise Manager itself, not related to device management

Enabling audit logging for device management events

Audit logs contain information about management operations performed from Enterprise Manager™ for a device, or for itself. Activities logged include creating a device alert, enabling a node, and so forth.

1. In the navigation pane, click **System** > **Logs** > **Configuration** > **Options**.
2. In the Audit Logging area at the bottom of the screen, for the **MCP** setting, select **Enable**.
3. Click the **Update** button.

Enterprise Manager creates an audit log entry any time it performs a change to a managed device.

Viewing and searching audit logs for device configuration changes

You must enable audit logging before you can view or search for events specific to device management.

From the Audit List screen, you can view or search any configuration changes you have made to the managed devices in your network. Use this information to monitor device management events and troubleshoot configuration issues.

1. On the Main tab, click **System** > **Logs** > **Audit** > **List**.
   The Audit List screen opens to display an overview of the activity for managed devices.
2. To search for a particular event, type a string in the **Search** field and click the **Search** button.

Viewing and searching Enterprise Manager system event logs

Enterprise Manager™ logs all system events specific to the operating system and other Linux components, not associated with Enterprise Manager software. This information is stored in the `/var/log/messages` file.

You can view the details derived from this data from the System Enterprise Management Logs screen.

1. On the Main tab, click **System** > **Logs** > **System**.
2. On the Menu bar, click **Enterprise Management**.
   The screen displays system events specific to Enterprise Manager.
3. To search for a particular event, type a string in the **Search** field and click the **Search** button.

Processes used for logging system events

The Enterprise Manager™ system uses the following processes for logging system events.

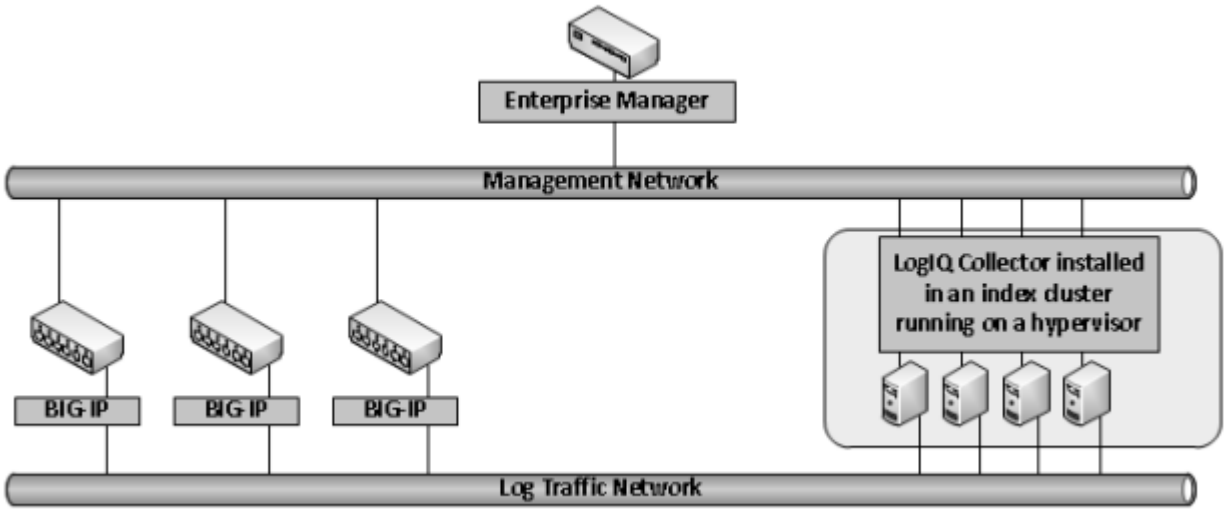
System process	This enables
emadmind	The scheduled Enterprise Manager ConfigSnyc feature
emalertd	Custom alerting features for managed devices, including creating alert instances, assigning alert actions, and logging alert events
emdeviced	Device management features such as managing device lists, performing high availability functions, and refreshing device status information
emfiled	Features required to manage device configuration archives, including scheduling a rotating archive schedule, and maintaining pinned archives
emrptschedd	Scheduled reports creation activities
swimd	Software image management features, including importing software or hotfix images to the software repository, and deploying software or hotfixes to managed devices

Overview: Collecting and aggregating log files with LogIQ

With LogIQ, you can view aggregated log events for all of your managed BIG-IP® devices from a centralized location and, with its powerful search tool, easily locate specific log events. LogIQ also provides you with the ability to increase storage as needed, by utilizing storage resources from your hypervisor.

You incorporate LogIQ into your network configuration by configuring two VLAN interfaces on your hypervisor. The first interface connects Enterprise Manager™ to the Management VLAN, and the second connects BIG-IP LTM® to the Traffic VLAN.

Figure 1: Standard implementation of LogIQ in your network



LogIQ components

The LogIQ feature is comprised of these components.

Component	Description
LogIQ Collector	The file that you download (`LogIQ-Collector<version>.ova`) and install on an ESXi hypervisor (on which storage has been allocated for the LogIQ Collector), and add to the index cluster for log event storage.
Index cluster	A collection of LogIQ Collectors on which you store log events.
Source devices	Managed BIG-IP® devices from which you collect log events.

About configuring LogIQ

To start collecting and aggregating log event files through LogIQ, you perform the following tasks.

- Configure two VLAN interfaces as follows:
  - A VLAN that connects to Enterprise Manager™ through the Management network interface
  - A VLAN that connects to the BIG-IP® LTM® through the Traffic network interface

  Important: *LogIQ is compatible only with BIG-IP LTM devices running version 11.3.0 and later.*

  For specific instructions about how to configure the hypervisor that is located in a network with a DHCP server, refer to your VMware ESXi hypervisor documentation.
- Download the LogIQ Collector `.ova` file and deploy it on your VMware ESXi hypervisor version 5.0.0, allocating sufficient storage space for your log indexing volume and retention requirements.
- Specify the default settings for the index cluster. (These settings apply to any LogIQ Collectors added to the index cluster.)
- Add the LogIQ Collector to the index cluster.
- Specify the source devices (managed BIG-IP® systems), from which to collect the data.
- Configure a network logging profile on the source device

Important: *The LogIQ feature is compatible only with the VMware ESXi hypervisor, version 5.0.0. By default, the LogIQ Collector is configured with 4 CPU cores, 4GB RAM, and 32GB system disk. You must add a new disk to retain logs in the ESXi hypervisor. If you add the disk while the LogIQ feature is running, you must reboot the system before Enterprise Manager can detect the new disk.*

Configuring IP addresses for VLAN interfaces from the command line

Before you can download and install LogIQ Collector, you must configure a management VLAN interface and a traffic VLAN interface. The LogIQ Collector is based on standard Linux CentOS distribution. Therefore, if you do not have a DHCP configured in your network to dynamically assign the IP addresses for the required interfaces, you can configure the IPV4 or IPV6 addresses from the command line.

Note: *If your network has a DHCP server, refer to your hypervisor documentation for instructions about how to configure the required VLAN interfaces.*

1. Log in to the hypervisor console screen as the `root` user.

   The default password is `default`.
2. To set addresses for your management and traffic VLANs, type the following commands: `# serviceConfig interface set Management <IP address/subnet mask> # serviceConfig interface set Traffic <IP address/subnet mask>`.
3. You can review the configuration by typing `# serviceConfig interface list`.

F5 recommends that at this point you change the default password using the `passwd` command.

Downloading the LogIQ Collector

You download the LogIQ Collector `.ova` file so that you can install it on an ESXi hypervisor for indexing and querying collected log events using the LogIQ feature.

1. From a web browser, navigate to the F5 Downloads page at `https://downloads.f5.com`.
2. Locate and download the EM LogIQ Collector package ending with `.ova`.
3. On your VMware client, deploy the `.ova` file.
4. Allocate a sufficient amount of storage for the LogIQ Collector from the hypervisor, as required by your log indexing volume and retention needs.

Specifying default settings for LogIQ Collector index clusters

It is important to specify default settings before you add a LogIQ Collector to the index cluster, because once you do, it is immediately available to index log events. If you make changes to these default settings after you have added LogIQ Collectors, the new changes overwrite the previous settings.

1. On the Main tab, click **Enterprise ManagementLogIQ** > **Index Cluster Config**.
2. In the **Maximum Days in Archive** field, specify the number of days that you want to keep collected log events.

   Note that if you change this setting to a smaller number in the future, the system may need to delete log entries to meet the newly reduced limit. Log event storage is dependent on disk space, regardless of the number of days specified.
3. Click the **Save** button, located directly below the **Maximum Days in Archive** setting.
4. To populate the **DNS and Time Configuration** settings with those configured for the Enterprise Manager system, click the **Load Local Settings** button located at the bottom of the screen. To specify alternative settings, complete steps 5-7.
5. For the **Domain Name Servers** setting, in the **Address** field, type the IP address of the DNS server that you want to use for the index cluster, and click the **Add** button.
6. From the **Timezone** list, select a time zone.
7. For the **Network Time Protocol Servers** setting, in the **Address** field, type the IP address of the FQDN of the NTP server, and click the **Add** button.
8. Click the **Save** button to change the default settings that you specified for the index cluster.

Adding a LogIQ Collector to the index cluster

You must download and configure the LogIQ Collector, allocate resources for the LogIQ Collector from your hypervisor, and configure the index cluster default settings before you add a LogIQ Collector to the index cluster.

When you add the first LogIQ Collector to the index cluster, it is available to index log events.

1. On the Main tab, click **Enterprise ManagementLogIQ** > **Index Cluster**.
2. Click the **Add Device** button.
3. In the **LogIQ Collector IP Address** field, type the IP address of the LogIQ Collector that you downloaded.
4. If you want the source device to use an IPV6 address (if available) for the traffic VLAN, select the **Use IPV6 address** check box.
5. Click the **Add** button.
6. The LogCollector you added displays in the index cluster table.
7. Click the address of the LogIQ Collector that you added.
8. In the Storage Devices list, select the check box next to an available device from which you can allocate storage for LogIQ.
9. Click the **Allocate storage** button.
10. In the dialog box that displays, click the **Add** button.

The LogIQ Collector you added to the index cluster displays in an up state, and is now available for index collection and log event indexing.

Next you must specify the source devices from which to collect log events.

Specifying a source device for LogIQ

The LogIQ feature indexes collected log events from the source devices that you specify.

1. On the Main tab, click **Enterprise Management** > **LogIQ** > **Source Devices**.
2. Click the **Add devices** button.
3. Use the **Device List** and **Device Filter** settings to specify which devices you want displayed.
4. Select the check box next to the source device for which you want to collect log events.
5. Click the **Add devices** button.

You must now configure a logging profile on the source device you specified, to use the **em-centlog-pub** publisher.

Configuring a network firewall logging profile on a source device

You can create a network firewall logging profile only after you add a LogIQ Collector to the index cluster and specify a source device.

Important: *To configure a network firewall logging profile, you must have Advanced Firewall (AFM) provisioned on the source device. You provision this on the* ***System*** > ***Resource Provisioning*** > ***Configuration****.*

When you create a logging profile, you specify the log events that you want collected by the LogIQ Collector.

1. On the Main tab, click **Security** > **Event Logs** > **Logging Profiles**.
2. Click the **Create** button.
3. In the **Profile Name** field, type a unique name to identify this logging profile.
4. For the **Network Firewall** logging profile setting, select the **Enabled** check box.
5. From the **Publisher** list, select **em-centlog-pub**.
6. Select the check box next to each type of log event that you want to log.
7. From the **Storage Format** list, select the format type that you want to use for the log events.
   a) If you want to use a delimiter to separate the fields, in the **Delimiter** field, type a value.
   b) From the **Available items** list, select the items that you want stored.
8. If you want to collect IP Intelligence log events, from the **Publisher** list, select **em-centlog-pub**.
9. Click the **Finished** button.

All specified log events are now collected and displayed on Enterprise Manager™.

Tip: *For additional information logging profiles, refer to the BIG-IP® Local Traffic Manager™ documentation specific to high-speed logging.*

About viewing and searching all collected log events

LogIQ features a powerful search tool that helps you easily locate specific log events. You can view all collected log events at once, or selected log events that occurred in a standard time period. You can also create your own customized time frame for which to view log events. These search options give you the flexibility to quickly find the information that you need.

Viewing all collected log events for a standard time period

You can view all of the log events that LogIQ has collected, or you can easily limit the number displayed by specifying a standard time period in which an event occurred.

1. On the Main tab, click **Enterprise Management** > **LogIQ** > **Search**.
2. From the **Time Period** list, select a standard period of time for which you want to view log events.
3. Click the **Update** button.

Enterprise Manager™ displays the events that LogIQ collected during the specified time period.

Viewing all collected log events for a custom time period

You can reduce the volume or range of collected events that are displayed by setting a custom time period for filtering.

1. From the **Time Period** list, select **Custom**.
2. Click in the **From** field.
   a) On the calendar, click the first day from which you want to view collected log events. Alternatively, click the **Now** button to populate the **From** field with the current date and time.
   b) For the **Hour**, **Minute**, and **Second** settings, move the slide bar to the right to specify the time of day to start displaying collected log events.

3. Click in the **To** field.
   a) On the calendar, click the last day for which you want to view collected log events. Alternatively, click the **Now** button to populate the **To** field with the current date and time.
   b) For the **Hour**, **Minute**, and **Second** settings, move the slide bar to the right to specify the time of day to stop displaying collected log events.
4. Click the **Update** button.

Enterprise Manager™ displays the events that LogIQ collected during the custom time period.

Creating a search filter for all collected log events

Before you can create a filter to look for specific entries, you must have configured LogIQ and have collected log events.

Log events provide you with information on which you need to act, as well as information to help you troubleshoot issues. You can use the LogIQ feature's sophisticated searching mechanism to filter log events by explicit attributes to help you find a specific event.

1. On the Main tab, click **Enterprise Management** > **LogIQ** > **Search**.
2. In the **New Filter** field, type a string that includes the field name and the specific data that you are searching for. The acceptable formats include those shown here.

Filter description	Search string example
Use quotation marks to filter for an exact match.	source_ip="10.10.10.1"
Not using quotation marks will return more results.	source_ip=10.10.10
To broaden the filter and increase the number of results, use the Boolean operator OR.	source_IP="10.10.10.1" OR source_IP="10.10.10.2"
To narrow the filter to an exclusive set of parameters, use the Boolean operator AND.	source_ip="10.10.10.1" AND dest_ip="192.168.1.1"

3. Optionally, place your cursor over an element in an event log and click it to add it to the search filter.
4. Click the **Add** button after each filter you create.
5. When you have added the last filter that you want to use, click the **Update** button.

The log event table refreshes to display only those events that include the filters that you specified.

About viewing and searching only network events

When you have LogIQ configured, you can view all collected logs or only those specific to the network. You also have the option to view all collected network log events at once, or selected network log events that occurred in a standard time period. Another option is to create your own customized time frame for which to view network log events. These search options give you the flexibility to quickly find the information that you need.

Viewing collected network log events for a standard time period

You can view all of the network log events that LogIQ has collected, or you can easily limit the number displayed by specifying a standard time period in which a network event occurred.

1. On the Main tab, click **Security** > **Event Logs** > **Network**.
2. From the **Time Period** list, select a standard period of time for which you want to view network log events.
3. Click the **Update** button.

Enterprise Manager™ displays the network log events that LogIQ collected during the specified time period.

Viewing collected network log events for a custom time period

You can reduce the volume or range of collected events that are displayed by setting a custom time period for filtering.

1. On the Main tab, click **Enterprise Management** > **LogIQ** > **Search**.
2. From the **Time Period** list, select **Custom**.
3. Click in the **From** field.
   a) On the calendar, click the first day from which you want to view collected log events. Alternatively, click the **Now** button to populate the **From** field with the current date and time.
   b) For the **Hour**, **Minute**, and **Second** settings, move the slide bar to the right to specify the time of day to start displaying collected log events.
4. Click in the **To** field.
   a) On the calendar, click the last day for which you want to view collected log events. Alternatively, click the **Now** button to populate the **To** field with the current date and time.
   b) For the **Hour**, **Minute**, and **Second** settings, move the slide bar to the right to specify the time of day to stop displaying collected log events.
5. Click the **Update** button.

Enterprise Manager™ displays the events that LogIQ collected during the custom time period.

Creating a search filter for collected network log events

Before you can create a filter to look for specific entries, you must have configured LogIQ and have collected log events.

Network log events provide you with information on which you need to act, as well as information to help you troubleshoot issues. You can use the sophisticated drag-and-drop method that Enterprise Manager™ provides to select specific log events and attributes as filters to find a precise event.

1. On the Main tab, click **Security** > **Network**.
2. Locate the log event, or log event element that you want to add to the custom search filter.
3. To add all of the elements of a single log event, hover over the first column of an log event table and drag it to the Custom Search field. Alternatively, you can hover over a single element in a log event and drag it to the Custom Search field.
4. When you have selected the last log event or element, click the **Update** button.

The log event table refreshes to display only those events that include the filters that you specified.

Chapter 5

Health and Performance Monitoring Statistics

Overview: Health and performance monitoring statistics

When statistics data collection is enabled, Enterprise Manager™ stores the following information in its statistics database for each managed device on which the Data Collection Agent is installed:

- Specifics about the managed devices, such as host name, IP address, and software version
- Details, such as object type and name, about any enabled network objects associated with a managed device
- Performance and health data for managed devices and associated network objects

You can use collected statistics to display standardized reports about the health and performance of managed devices in your network. This helps you identify any systems that are not performing at full capacity and assists you in determining when you should add new devices.

Important: *Enterprise Manager collects statistics only from devices that have BIG-IP® Local Traffic Manager™ licensed and provisioned. Starting with Enterprise Manager version 2.3, Enterprise Manager can also collect statistics from devices licensed and provisioned for BIG-IP Global Traffic Manager™.*

To start collecting statistics, you must enable the collect statistics data feature and install the Data Collection Agent.

Enabling statistics data collection

To collect statistics you must enable data collection, which is disabled by default.

Important: *Due to the processing power required to collect and store statistics data, only Enterprise Manager™ 4000 platform and Enterprise Manager Virtual Edition (VE) support statistics data collection. If you are upgrading from a version of Enterprise Manager that is earlier than 1.7, you must re-license the system before enabling data collection.*

Tip: *If Enterprise Manager is managing devices that are part of a BIG-IP® Global Traffic Manager™ (GTM™) synchronization group, Enterprise Manager temporarily disrupts communication between GTM and remote BIG-IP objects while it verifies the version of the* `big3d` *agent on GTM. To reduce the impact to production traffic relying on the BIG-IP GTM infrastructure, we recommend that you enable statistics data collection during a maintenance window. Alternatively, you can configure the BIG-IP GTM system to maintain an available status for the virtual servers on each managed device while communication is briefly disrupted.*

---

1. On the Main tab, click **Statistics** > **Options** > **Data Collection**.
2. For the **Collect Statistics Data** setting, select **Enabled**.
3. Click the **Save Changes** button.

When you enable statistics collection, Enterprise Manager verifies that each managed device has a compatible version of the Data Collection Agent installed.

Installing the Data Collection Agent

When data collection is enabled, Enterprise Manager™ collects health and performance monitoring statistics data for each managed device in your network on which the most current version of the Data Collection

Agent is installed. If a device on which statistics is enabled requires a more recent version of the Data Collection Agent, Enterprise Manager displays that device as `Impaired` in the device list, and indicates that an upgrade is required.

You can use the Data Collection Agent Installation wizard to update and install the Data Collection Agent.

1. On the Main tab, click **Enterprise Management** > **Tasks** > **Task List**.
2. Click the **New Task** button.
3. For the **Software Installation** setting, click **Install Data Collection Agent**, and then click **Next**.
   The Data Collection Agent Installation screen opens.
4. For the **Device Filter** setting, click the **Devices with data collection enabled requiring update** option.
   The screen refreshes to display the devices that require an update.
5. Select the check box next to each device on which you want to install the most recent version of the Data Collection Agent, and click **Next**.
   The Task Options screen opens.
6. From the **Configuration Archive** list, select an option to include or exclude private SSL keys in the configuration archive.
7. From the **Device Error Behavior** list, select an option to specify how you want the system to proceed if an error occurs during the Data Collection Agent installation task.
8. Click **Next**.
   The Task Review screen opens.
9. In the **Task Name** field, you can type a new name to customize the name that displays in the task list.
10. Click the **Start Task** button.
    The Task Properties screen opens, displaying the progress of the task. The task progress displays as Finished when the Data Collection Agent is installed.

Enterprise Manager starts collecting and storing health and performance monitoring statistics for the devices on which data collection is enabled and the Data Collection Agent is installed.

About statistics profiles

A *statistics profile* defines the specific performance monitoring statistics information that you want Enterprise Manager™ to collect, such as bytes and packets, connections, CPU utilization, memory, and disk usage. The statistics profile types correspond to the type of object that you want to monitor.

To collect performance monitoring statistics, assign one or both of these profile types, to the managed objects in your network.

Standard statistics profiles

A *standard statistics profile* contains all the required metrics that Enterprise Manager must collect for a specific network object type, to successfully create standard reports.

Custom statistics profiles

A *custom statistics profile* allows you to define your own metrics and optional threshold values for an object. By enabling or disabling data collection for certain metrics, you can prioritize the information you are collecting, ensuring that system resources are allocated appropriately.

Statistics data collected for the standard statistics profiles

When statistics collection is enabled, Enterprise Manager™ collects the following statistics data to create standard reports.

Report name	Statistics data collected for this report
Certificate Inventory	None
Device Inventory	None
Capacity Planning	• Device CPU - Processor Utilization (%) • Device Global Memory Utilization (%) • Device Global Client: Bits In (/Sec) • Device Global Client: Bits Out (/Sec)
Flapping Node	None
Flapping Pool Member	None
GTM Object Activity	• GTM Virtual Server Bits In (Ave per Sec) • GTM Virtual Server Bits Out (Ave per Sec) • GTM Virtual Server Connections (Ave per Sec)
LTM Node Inventory	None
SSL TPS Usage	• Device Client SSL Native Connections (per Sec) • Device Client SSL Compat-mode Connections (per Sec)
LTM Object Activity	• LTM Node Bits In (per Sec) • LTM Node Bits Out (per Sec) • LTM Pool Member Bits In (per Sec) • LTM Pool Bits In (per Sec) • LTM Pool Bits Out (per Sec) • LTM Virtual Server Bits In (per Sec) • LTM Virtual Server Bits Out (per Sec)
LTM Unused Object	• LTM Node Bits In (per Sec) • LTM Node Bits Out (per Sec) • LTM Pool Member Bits In (per Sec) • LTM Pool Bits In (per Sec) • LTM Pool Bits Out (per Sec) • LTM Virtual Server Bits In (per Sec) • LTM Virtual Server Bits Out (per Sec)

Creating a custom statistics profile

Before Enterprise Manager™ can monitor a device, you must enable statistics collection for that device.

In most cases, a standard statistics profile is best for monitoring objects in your network. With a custom statistics profile, however, you can specify your own minimum and maximum thresholds for a number of object-specific options, providing the flexibility to specify fewer or more metrics to monitor.

1. On the Main tab, click **Statistics** > **Managed Devices** > **View**.
2. From the menu bar, select a profile type based on the type of network object for which you are creating a statistics profile.
   - **Device Profiles**
   - **Global Traffic Profiles**
   - **Local Traffic Profiles**

The Profiles screen specific to that network object type opens.

3. Click the **Create** button.
   The New Profile screen opens.
4. From the **Profile Source** list, select an option.

Option	Description
Standard Profile	Select this option if you want to base the custom statistics profile on the metrics currently assigned to the standard profile for this network object type.
None	Select this option if you want to choose from all metrics available for this network object type.

   The **Profile Metrics** table refreshes to display the metrics associated with the source profile you selected.
5. In the **Name** field, type a name for this customized profile.
6. In the **Description** field, type details to help you identify this customized profile.
7. From the **Collection Interval** list, select the number of seconds that you want Enterprise Manager to collect metrics.
8. In the Profile Metrics table, select the **Collect Data** check box next to each metric that you want to collect.

Important: *If you selected the **Standard Profile** on which to base the custom statistics profile you are creating, you can select additional metrics to collect, but you must retain the current metrics for standard reports to run successfully. If you disable metrics required for standard reports, the report results will be invalid.*

---

9. In the metric's associated **Minimum Threshold** and **Maximum Threshold** fields, type the values the metric must reach for it to display as red in the graph.

   These values are optional. You are not required to specify a minimum or maximum threshold value to collect statistics for any metric.
10. Click **Save Changes**.

To start using this customized statistics profile, you must assign it to specific network objects, or set it as the default for newly discovered devices.

Assigning a statistics profile to a specific device or network object

Before Enterprise Manager™ can monitor a device, you must enable statistics collection for that device.

Assigning a statistics profile specific to objects in your network makes it easy for you to monitor performance based on standardized settings for that object, or customized settings that you specify.

1. On the Main tab, click **Statistics** > **Managed Devices** > **View**.
2. Click the name of the device for which you want to assign a statistics profile.
3. On the menu bar, click **Statistics** > **Configure**.
4. Verify that the **Collect Statistics Data** option is set to **Enabled**.
5. From the **Object Type** list, select the object to which you want to assign a statistics profile.
   The screen refreshes to display the objects for the selected object type.
6. From the **Associated Filter** list, select an option to further filter the objects that you want displayed.
7. Next to the object for which you want to assign a statistics profile, from the **Associated Profile** list, select a standard statistics profile or custom statistics profile for that object type.

8. Click **Save Changes**.

Enterprise Manager begins to collect statistics and report performance based on the selected profile.

Specifying a default statistics profile for newly discovered devices

Before Enterprise Manager™ can monitor a device, the device must be enabled for statistics collection.

You can assign a default profile (either a standard statistics profile or a custom statistics profile) to start monitoring devices as soon as Enterprise Manager discovers them in your network.

1. On the Main tab, click **Statistics** > **Managed Devices** > **Device Profiles**.
2. From the **Profile Name** list, select the profile that you want to use as the default for any newly discovered devices.
3. Click **Save Changes**.

Enterprise Manager applies the profile you selected to any newly discovered devices.

About network object statistics

With Enterprise Manager™, you can easily monitor the health and activity of managed objects in your network through collected statistics. You can view activity in a summary and detailed graph format. This information ensures that your network is performing efficiently and helps you to troubleshoot potential issues. Viewing statistics provides you with an overview and details about the health and activity of the objects in your network. You can customize the information displayed in the graphics on this screen by using rule classes. This flexibility provides you the at-a-glance view, while highlighting the statistics you are most interested in.

Displaying network object statistics and customizing view

You must have statistics collection enabled for a network object for Enterprise Manager™ to collect and display statistics.

You can view network activity based on collected statistics in a standardized or customized format.

1. On the Main tab, click **Statistics** > **Managed Devices** > **View**.
2. From the **Object Type** list, select the object type for the statistics that you want to view.
   The screen refreshes to display the related statistics in a summary graph. If no statistics exist for the object type you selected, the **Data** column displays **No Data**.
3. From the **Rule** list, select a rule class to specify the particular statistics displayed.
   The screen refreshes to display the associated statistics details in the summary graph.
4. From the **Time Span** list, select a range of time for which to display data.
5. Move the cursor over a graph to display a summary, or click the graph to view a detailed graph.

Rule class descriptions

The statistics data displayed is defined by the associated rule class.

Rule Class	Description
All Active	All statistics currently configured in the associated statistic profile
All Errors	All statistics related to error conditions
Commonly Used	A subset of commonly used statistics available in the associated statistic profile
Common Errors	A subset of commonly occurring errors available in the associated statistic profile
Device Health	A subset of device statistics related to the physical health of the device
Device Stats	A subset of device statistics related to the traffic management of the device
HTTP Stats	A subset of statistics related to HTTP traffic
Out of Range	A collection of statistics where the value is currently exceeding a user-set threshold
Red Line	A collection of resource-utilization statistics that have a user-set threshold
SSL Stats	A subset of statistics related to SSL traffic
TCP Stats	A subset of statistics related to TCP traffic
UDP Stats	A subset of statistics related to UDP traffic

Modifying the number of records per screen to display

By default, Enterprise Manager displays up to 10 records per screen. If there are more than 10 graphs, the screen displays a link where you can view additional graphs. If you want to view more than 10 records per screen, you can increase the number displayed. This global setting affects all list screens on the Enterprise Manager system. Performance can be affected the large number of items to display on a screen.

1. On the Main tab, click **System** > **Preferences**.
   The Preferences screen opens.
2. In the **Records Per Screen** field, type a new value.
   This is a global setting and that affects all screens that lists records.
3. Click the **Update** button.

About statistics storage

Enterprise Manager™ stores statistical data until the system reaches the storage capacity, which is by default, 1 GB stored locally. When this capacity is met, the oldest data in the system is replaced with new data, up to the storage limit. This default amount is intentionally low because when you enable statistics collection it affects the overall performance of the system. Therefore, it is important to plan for your database storage needs by understanding your system's capacity and personalize your storage requirements so you can maximize the value of the statistics features. Once you have estimated the availability of storage on your system, you can change the default database storage capacity setting. Increasing the default setting is essential to monitoring statistics data over time.

To help you plan for statistics storage, you can view the system's hard drive allocation by file type to remove any unnecessary files and calculate statistics data storage.

Viewing hard drive storage allocation

The Enterprise Manager™ system hard drive contains all locally-stored statistical data as well as software images, attack signature files, system logs, archives, and so forth. It is important to note that if you are collecting statistics for a large number of devices and objects, the size of the statistics database can be limited by how many other parts of the Enterprise Manager system are using the shared file system. You can view file allocation to determine if storage is maximized for your needs.

1. In the navigation pane, click **System** > **File System Management** > **File System Information**.
2. Review the storage allocation to identify any outdated or unnecessary file storage.

You can remove any superfluous files to free storage space to increase statistics data storage.

Calculating and modifying statistics storage allocation

When Enterprise Manager™ is configured to collect statistical data, the Data Storage screen displays a system-generated estimate of the number of days until the system reaches capacity for statistical data storage.

This number is calculated based on the current rate of data collection and the amount of disk space you specified for the storage space allocation. To retain more or less historical data, you can change the storage allocation space. To help you determine how much disk space you want to allocate to statistics storage, you can recalculate the estimated number of storage days by modifying the storage space. When you have determined that you are satisfied with the storage space value, you can then opt to save the changes.

1. On the Main tab, click **Statistics** > **Managed Devices** > **Options** > **Data Storage**.
2. From the **Allocated Statistic Storage Space** list, select a value for the number of gigabytes on the external database hard drive.
3. Click **Recalculate**.
4. Review the value displayed for the **Estimated Statistics Storage Capacity With Current Settings** setting.
5. Continue to change the **Allocated Statistic Storage Space** value until you are satisfied with the number of days for the estimated statistics storage.

   Important: *If you change the **Allocated Statistic Storage Space** setting to a value less than the current value, Enterprise Manager removes statistics data from the database, starting with the oldest, until it reaches the new lowered storage limit. For external databases, this value cannot exceed the available amount of disk space of the system on which you set up the external database. Enterprise Manager does not monitor the amount of disk space on the external database.*

   ---

6. Once you are satisfied with the number of days statistics are stored, click **Save Changes**.

Enterprise Manager allocates the specified hard drive space to statistics storage.

About statistics database backup and restoration

You can backup and restore the statistics database from the command line, or you can create a task to backup the statistics database on a regular schedule.

Scheduling statistics database backups

You must enable statistics collection and have content saved to the statistics database, before a scheduled backup can occur.

Scheduling a regular backup for you statistics database ensures you have a the option to restore it in the event of a system failure.

1. On the Main tab, click **Enterprise Manager** > **Tasks** > **Schedules** > **Statistics Database Backup**.
2. From the **Backup Data** list, select the frequency that you want Enterprise Manager to back up the statistics database.
   Depending on your selection, the screen refreshes to display associated options.
3. Specify the day of the week or month, and the time of day that you want Enterprise Manager to review the device's configuration for any changes.
4. In the **Username** field, type the user ID that you use to log in to the remote system.
5. In the **Hostname** field, type the FQDN of the remote system.
6. In the **Path** field, type the file path of the remote system.
7. Click **Save Changes**.

If any changes occur during the specified time frame, Enterprise Manager™ backs up the statistics database.

About external storage for health and performance monitoring statistics

By default, Enterprise Manager™ stores health and performance monitoring statistics data in the database located on its hard drive. You have the option of configuring Enterprise Manager to store these statistics on a hard drive that is separate (external) from the Enterprise Manager system. Storing statistics on an external database clears space on Enterprise Manager for more storage of archives, images, configuration files, and so forth. A space dedicated only to health and performance monitoring statistic data can also provide you with more historical data storage.

To use an external database for health and performance monitoring statistics storage, you must create the external database and then configure Enterprise Manager to store data on that database.

If you previously collected data locally on the Enterprise Manager system, you have the option to back up and restore the data to the external database.

Task summary

Creating an external database for health and performance monitoring statistics
Backing up a local statistics database to an external statistics database
Configuring Enterprise Manager to store statistics to an external database
Backing up and restoring an external statistics database

Creating an external database for health and performance monitoring statistics

Storing statistics on an external database clears space on Enterprise Manager™ for more storage of archives, images, configuration files, and so forth. A space dedicated only to health and performance monitoring statistics can also provide you with more historical data.

You create an external database for statistics storage by issuing SQL commands on a system that is running Oracle® MySQL®version 5.1 with patch 52 or later.

Important: *To avoid potential time-out issues, start the MySQL instance using the* `--skip-name-resolve` *option.*

1. Access the command line of a system that is running Oracle® MySQL® version 5.1 with patch 52 or later.

   For specific information about the following commands, refer to your *MySQL Reference Manual*.
2. Type: `create database <database>` , where `<database>` is the name of the external database.
3. Type: `grant all privileges on <database>.* to <username>@<host> identified by <password>` , where `<host>` includes the IP address of the Enterprise Manager system that is storing data on the external database and `<password>` is the password for the user name specified.
4. Type: `grant select on mysql.proc to <username>@<host>`.

   This command sets privileges so that the specified user can initiate the required procedures for Enterprise Manager to store and access data on the external database.
5. Type: `set global log_bin_trust_function_creators = 1`.

   This command relaxes the privilege conditions so that Enterprise Manager can create necessary functions and procedures that enable you to store and access statistics data.

You should now edit the MySQL configuration file to optimize the database and avoid potential memory issues.

Backing up a local statistics database to an external statistics database

If you previously collected data locally on the Enterprise Manager™ system, you can back up and restore the local data to the external database that you created.

1. On the Main tab, click **Statistics** > **Managed Devices** > **Options** > **Data Collection**.
2. From the **Collect Statistics Data** list, select **Disabled**.
3. Click the **Save Changes** button.
4. On the system on which the local database is located, create a back up of the data by running the following command: `mysqldump -u <user> -p -R f5em_extern> dump.sql`, where `<user>` is the user name assigned to the database.
5. On the system on which you created the external database, restore the data by running the following command: `mysql -u <user> -p -D remotedb < dump.sql`, where `<user>` is the user name assigned to the database.
6. On the Main tab, click **Statistics** > **Managed Devices** > **Options** > **Data Collection**.
7. From the **Collect Statistics Data** list, select **Enabled**.
8. Click the **Save Changes** button.

You can now configure Enterprise Manager to store health and performance monitoring statistics on the external database.

Configuring Enterprise Manager to store statistics to an external database

After you have created the external database on the remote system, you can configure Enterprise Manager™ to store data there.

Configuring Enterprise Manager to store health and performance monitoring statistics on an external database frees system resources, and provides you with space to store statistics that is limited only by the system's hard drive on which you configure the external database.

Important: *When configured to use an external database for statistics storage, Enterprise Manager no longer monitors, reports, nor sends alerts regarding storage capacity and usage, and you cannot schedule or perform statistics database backups and restorations from Enterprise Manager. When statistics are stored in an external database, the administrator of the remote system on which the statistics are stored must perform capacity management, and backup and restoration tasks independently of Enterprise Manager.*

If you have two Enterprise Manager systems configured as a high availability system, configure the external database the same way on each system.

1. On the Main tab, click **Statistics** > **Managed Devices** > **Options** > **Data Storage**.
2. For the **Statistics Data Location** setting, select **External**.
   The screen refreshes to display additional fields specific to the external database option.
3. In the **External Database Address** field, type the IP address of the system on which you configured the external database.
4. In the **External Database Port** field, leave **3306** for the MySQL default port, or type a new port number in the field.
5. In the **External Database Name** field, type a name for the external database.
6. In the **External Database User** and **External Database Password** fields, type the credentials required to access the database.
7. In the **Allocated Statistic Storage Space** field, type a value for the number of gigabytes (GB) that you want to dedicate to storing statistics.

   This value cannot exceed the available amount of disk space of the system on which you set up the external database. Enterprise Manager does not monitor the amount of disk space on the external database.
8. Click **Save Changes**.
   The screen displays a summary of the configuration.
9. If the summary details are correct, click **Confirm** to initialize the configuration.

When the configuration changes are fully initialized, Enterprise Manager begins to store health and performance monitoring statistics data in the external database. (This transition may take a few minutes.) Content currently stored in the local database remains there until you remove it.

Removing local statistics data storage

After you configure Enterprise Manager™ to store health and performance monitoring statistics on an external database location, you can remove the data stored locally to free more disk space. Before removing the local statistics, first verify that external statistics storage, data retrieval, and reporting functionality are working as expected, and that the locally-stored data is no longer useful or relevant. Or, if you want to retain the local data, back up the local data to store elsewhere, prior to deleting it.

Removing the locally-stored statistics increases the amount of storage that Enterprise Manager can use for archives, images, configuration files, and so forth.

1. On the Main tab, click **Statistics** > **Managed Devices** > **Options** > **Data Storage**.
2. Click the **Delete Local Statistics Data** button.
3. Click **Confirm**.

Enterprise Manager frees the local disk space that was previously dedicated to storing statistics data.

Backing up and restoring an external statistics database

Enterprise Manager™ cannot run scheduled backups and restoration for statistics stored on an external database. When statistics are stored on a remote system, the administrator of must perform backup and restoration tasks independently of Enterprise Manager.

About external storage for health and performance monitoring statistics
Configuring Enterprise Manager to store statistics to an external database
Backing up an external statistics database
Backing up an external statistics database
Restoring the external statistics database

Backing up an external statistics database

You must enable statistics collection and have content saved to the configured external statistics database, before you can create a backup.

If you created an external database for health and performance monitoring statistics storage, you must manually back up that database for archive and restoration purposes.

1. Log in to the Enterprise Manager™ command line as `root`.
2. Type the `em-backup-extern <user@host.com>:/>full_file_path_for_backup_file>` command.

   The default file name is `f5em_extern-<date stamp>`.

Enterprise Manager saves the stored contents of the external statistics database to the specified file.

Backing up and restoring an external statistics database

Restoring the external statistics database

You must backup the external statistics database before you can restore it.

If you have configured an external database on which to store statistics, and you want to restore data that you have backed up, you must do that from the command line.

1. Log in to the Enterprise Manager™ command line as `root`.
2. Type the `em-restore-extern <user@host.com>:/>full_file_path_for_backup_file>` command.

   For example: `em-restore-extern <user@host.com>f5em_extern-<date stamp>`.

Enterprise Manager restores the backed-up content of the external statistics database to the specified location.

Backing up and restoring an external statistics database

About reports

You can use Enterprise Manager™ reports to retrieve and view information about the devices and BIG-IP® Local Traffic Manager™ (LTM®) and BIG-IP Global Traffic Manager™ (GTM™) objects in your network. To create a report, you define parameters, the devices from which to collect the data, and the object types you want to include. You can collect data and view the report immediately, or you can schedule the report to run in the future either once, or at regular intervals. Depending on the report type, completed reports are presented in Adobe® portable document format (PDF) or comma-separated value (CSV) text, which you can export to a spreadsheet, such as Microsoft® Excel®. The Capacity Planning report also supports an interactive HTML format.

Important: *Before you can use the reports feature, you must enable data collection. You have the opportunity to enable data collection when you create a report. However, if you upgraded to the current version of Enterprise Manager from a version prior to 1.7, you must re-license the system before you can enable data*

collection. Due to the processing power required to collect and store statistical information, data collection is available only for the Enterprise Manager 4000 platform.

Standard reports

This table outlines the standard reports that you can create using Enterprise Manager™.

Table 1: Enterprise Manager report descriptions

Report name	Description	Use this report to	Format
Capacity Planning	Performance capacity details about CPU usage, memory usage, and throughput	To help you identify devices that are running near the edge of capacity and to make any required changes	PDF and HTML
Certificate Inventory	Information about the SSL certificates for the devices that Enterprise Manager has discovered in your network	Easily manage multiple SSL certificates and identify those that have expired, or are about to expire	CSV
Device Inventory	Comprehensive details about the devices that Enterprise Manager has discovered in your network	Centrally manage all of the details of the managed devices in your network	CSV
Flapping LTM Node	A list of Local Traffic Manager™ (LTM®) nodes that repeatedly restart, going from an up state to a down state and back again (referred to as *flapping*)	Identify and troubleshoot potential issues with the connectivity to nodes in your network	PDF
Flapping LTM Pool Member	A list of pool members that repeatedly restart, going from an up state to a down state and back again.	Identify and troubleshoot potential issues with the connectively to pool members in your network	PDF
GTM Object Activity	Global Traffic Manager™ (GTM™) object activity details	Monitor the activity and performance of GTM objects in your network, troubleshoot potential issues, and reallocate resources as needed	PDF
LTM Node Inventory	The names of nodes that Enterprise Manager has discovered in your network	Manage the status and state of all of the nodes in your network	PDF
LTM Object Activity	Local Traffic Manager (LTM) object activity details	Monitor the activity and performance of LTM objects in your network, troubleshoot potential issues, and reallocate resources as needed	PDF
SSL TPS Usage	SSL certificate transactions per second (TPS) for each device	Monitor SSL certificate activity trends for your	PDF

Report name	Description	Use this report to	Format
	that Enterprise Manager has discovered in your network	devices, and to plan for platform upgrades and future transition to 2K bit SSL certificate keys	
Unused LTM Objects	All Local Traffic Manager (LTM) objects that have had no activity within a configured date parameter	Monitor the activity of LTM objects in your network, troubleshoot potential issues, and reallocate resources as needed	PDF

Creating reports

You can create Enterprise Manager™ reports to easily manage details about the objects associated with the managed devices in your network.

1. On the Main tab, click **Enterprise Management** > **Reports**.
   The Reports screen opens.
2. Under **Types**, click the report type that you want to create.
   The screen refreshes, displaying any currently configured reports of the selected type that are scheduled, or have run.
3. Click the **Create** button.
   The Report Options screen opens, displaying the settings relevant to the type of report you are creating.
4. In the **Name** field, type the name as you would like it to appear on the report, and on the scheduled and completed report list.
5. If you are creating a Certificate Inventory or Device Inventory, click the **Next** button and follow the steps in the *Scheduling reports* procedure.
6. For the remainder of the reports, specify settings for the report, then click the **Next** button and then follow the steps in the *Scheduling reports* procedure. For specific information about each report setting, refer to the online help.

Report options

The report options vary depending on the type of report that you are creating.

You can specify values for the following settings when creating a Capacity Planning report.

Capacity Planning report setting	Default value	Action
Aggregation Interval	No default value	Specify the interval over which the data is averaged, to find the maximum capacity reached during the data collection period.
Filter	N/A	To restrict the number of devices displayed, type a full or partial name or IP address in the field, and click the **Filter** button.
Device Name	No default value	Select the check box next to the devices from which you want to collect data. You must select at least one device.

Capacity Planning report setting	Default value	Action
Memory headroom (%)	85	Specify the maximum memory threshold to use for calculating the projected date that the capacity limit is reached.
CPU headroom (%)	85	Specify the maximum CPU threshold to use for calculating the projected date that the capacity limit is reached.
Throughput headroom (bits/sec)	1000000	Specify the maximum throughput threshold to use for calculating the projected date that the capacity limit is reached.

You can specify values for the following settings when creating a Certificate Inventory report.

Flapping LTM Node report setting	Default value	Action
Interval (minutes)	30	Specify the period of time within which to check for flapping nodes.
Threshold (count)	2	Specify the minimum number of times during the interval that a node must flap before it is included in the report.
Filter	N/A	To restrict the number of devices displayed, type a full or partial name or IP address in the field, and click the **Filter** button.
Device Name	No default value	Select the check box next to the devices from which you want to collect data. You must select at least one device.

You can specify values for the following settings when creating a Flapping LTM® Pool Member report.

Flapping LTM Pool Member report setting	Default value	Action
Interval (minutes)	30	Specify the period of time within which to check for flapping pool members.
Threshold (count)	2	Specify the minimum number of times during the interval that a pool member must flap before it is included in the report.
Filter	N/A	To restrict the number of devices displayed, type a full or partial name or IP address in the field, and click the **Filter** button.
Device Name	No default value	Select the check box next to the devices from which you want to collect data. You must select at least one device.

You can specify values for the following settings when creating a GTM™ Object Activity report.

GTM Object Activity report setting	Default value	Action
Max number of objects	10	Specify the maximum number of objects that you want displayed in the report.
Most or Least Active	Most Active	From the list, select an option to display the most active or the least active objects.
Filter	N/A	To restrict the number of devices displayed, type a full or partial name or IP address in the field, and click the **Filter** button.

GTM Object Activity report setting	Default value	Action
Device Name	No default value	Select the check box next to the devices from which you want to collect data. You must select at least one device.

You can specify values for the following options when creating an LTM Node Inventory report.

LTM Node Inventory report setting	Default value	Action
Filter	N/A	To restrict the number of devices displayed, type a full or partial name or IP address in the field, and click the **Filter** button.
Device Name	No default value	Select the check box next to the devices from which you want to collect data. You must select at least one device.

You can specify values for the following settings when creating an LTM Object Activity report.

LTM Object Activity report setting	Default value	Action
Max number of objects	10	Specify the maximum number of objects that you want displayed in the report.
Most or Least Active	Most Active	From the list, select an option to display the most active or the least active objects.
Show Object	All object types	Clear the check box next to the object type for which you do not want to collect data.
Filter	N/A	To restrict the number of devices displayed, type a full or partial name or IP address in the field, and click the **Filter** button.
Device Name	No default value	Select the check box next to the devices from which you want to collect data. You must select at least one device.

You can specify values for the following options when creating an SSL TPS Usage report.

SSL TPS Usage report setting	Default value	Action
Filter	N/A	To restrict the number of devices displayed, type a full or partial name or IP address in the field, and click the **Filter** button.
Device Name	No default value	Select the check box next to the devices from which you want to collect data. You must select at least one device.

You can specify values for the following options when creating an Unused LTM Objects report.

Unused LTM Objects report setting	Default value	Action
Show Object	All object types	Clear the check box next to the object types for which you do not want to collect data.

Unused LTM Objects report setting	Default value	Action
Filter	N/A	To restrict the number of devices displayed, type a full or partial name or IP address in the field, and click the **Filter** button.
Device Name	No default value	Select the check box next to the device from which you want to collect data. You must select at least one device.

Scheduling reports

You must specify values for the Report Options settings before you can schedule the report.

You can schedule a report to run immediately, providing you with a current snapshot of your inventory or activity, or you can schedule the report to run in the future either once, or at regular intervals.

1. On the Main tab, click **Enterprise Management** > **Reports**.
   The Reports screen opens.
2. Under **Types**, click the report type that you want to schedule.
   The screen refreshes, displaying any currently configured reports of the selected type that are scheduled, or have run.
3. For the **Run this report** setting, select an option from the list to specify when, or at what interval, to run the report.

   Keep in mind that frequent data collection requires more storage space, which reduces the total amount of historical data that you can keep.

   The settings on the screen change, depending on the option you select.
4. If you selected an option other than **Now** for the **Date and Time** setting, specify the date and time that you want to run the report.
5. If you are creating a Flapping Nodes, LTM Object Activity, or Unused LTM Objects report, for the **Date Collection Interval** setting, specify the amount of time (prior to the report run date) to collect data.
6. To specify a person to receive this report by email, in the **Email Subscription** field, type the email address of the person and click **Add Email**.
7. Repeat the previous step for each additional email recipient you want to add.
8. To remove an email address, select the check box next to the email address, and click **Remove**.
9. Click the **Submit** button to save your changes.
   The Reports screen opens, displaying the report in the Scheduled Reports area or the Completed Reports area, depending on when it is scheduled to run.

Viewing and downloading reports

After Enterprise Manager™ has collected the specified data for a report, it lists the report in the Completed Reports area of the associated Reports screen. When the report is displayed in this area, you can view it as well as can download the report for distribution or archival.

1. On the Main tab, click **Enterprise Management** > **Reports**.
   The Reports screen opens.
2. Under **Types**, click the report type that you want to view.

The screen refreshes, displaying any currently configured reports of the selected type that are scheduled, or have run.

3. Select the check box next to the report that you want to view, and click the **Download** button.
   You are prompted to open or save the file.
4. Click the **Open** button to view the report immediately.
   Optionally, you can click the **Save** button and navigate to a place to save the file.

Viewing the interactive HTML version of the Capacity Planning report

After Enterprise Manager™ has gathered the specified data for a Capacity Planning report, it lists the report in the Completed Reports area. When the report is displayed in this area, you can view the interactive HTML version. When you view the HTML version of this report, you can modify the settings to instantly display updated capacity projection end dates. Alternatively, you can save the report as a static PDF file, as you do all other Enterprise Manager reports.

Note: *The Capacity Planning report is the only report available in interactive HTML format.*

1. On the Main tab, click **Enterprise Management** > **Reports**.
   The Reports screen opens.
2. Under **Types**, click **Capacity Planning**.
   The screen refreshes to display any configured Capacity Planning reports that are scheduled, or have run.
3. Select the check box next to the Capacity Planning report that you want to view, and click the **View** button.
   The Capacity Planning report you selected displays.
4. If you have configured this report to run for more than one device, you can select another device from the **Capacity Planning for** list to view the associated report.
5. To modify the headroom for CPU, memory, or throughput metrics, type a new value in the associated **Headroom** field and click the **Update Projection** button.
   The report refreshes to display the updated end date projection based on the new value.
6. To change the type of statistical analysis method, select one of the following options from the **Projection Type** list.

Option	Description
No Regression	Displays the usage trends for the associated metrics and does not project a run out date.
Linear	Uses the least squares linear regression analysis method, which takes into account all historical data and minimizes any deviations to calculate a projected run out date.
Holt-Winters	Uses the exponential smoothing forecasting method, which takes the most recent data more into consideration to calculate a projected run out date.

Modifying report settings

You can modify the settings for a report only if it is scheduled to run at some time in the future.

After a report is scheduled, you can change the report name, how often the report runs and, if applicable, the devices from which to collect data.

1. On the Main tab, click **Enterprise Management** > **Reports**.
   The Reports screen opens.
2. Under **Types**, click the report type that you want to modify.
   The screen refreshes, displaying any currently configured reports of the selected type that are scheduled, or have run.
3. Select the check box next to the report that you want to modify.
4. Click the **Edit** button.
   The Report Options screen opens.
5. Modify the settings as required.
6. Click the **Submit** button to save your changes.
   The Reports screen opens, displaying the report in the Scheduled Reports area or the Completed Reports area, depending on when it is scheduled to run.

Report components

The components of each report vary depending on the report type.

Capacity Planning report components

- Device name
- Device IP address
- Metric (CPU, memory, throughput)
- Peak value
- Projected run out date range

Certificate Inventory report components

- Device name
- Certificate name
- Certificate type
- Key type
- Version
- Serial number
- Certificate expiration date
- File name
- Bit length
- Management mode
- Common name
- Certificate organization
- Certificate division

- Certificate country
- Certificate state
- Certificate locality
- Issuer organization
- Issuer division
- Issuer country
- Issuer state
- Issuer locality

Device Inventory report components

- Device name
- Device IP address
- System ID
- Configuration utility address
- Management port address
- Management interface address
- Management netmask address
- Management gateway address
- Enterprise Manager server IP address
- Enterprise Manager IP address
- Clock skew data
- Time zone
- Uptime (hours:minutes)
- Platform identification
- Serial number
- Failover state
- Failover mode
- Failover forced active
- Peer state
- Configuration synchronization status
- Last configuration date
- Last configuration synchronization date
- Last refresh date
- User authentication URL
- Shell access status
- Shell access filter
- Device location
- Device contact information
- Active boot (slot) location
- Service contract end date
- Software product
- Software version
- Software build number
- Base registration key

Flapping LTM Node report components

- Node IP address
- Device name
- Flap start date and time

- Flap end date and time
- Final state of node
- Flap number

Flapping LTM Pool Member report components

- Pool IP address
- Device name
- Flap start date and time
- Flap end date and time
- Final state of pool
- Flap number

GTM Object Activity report components

- Virtual server name
- Device name
- Bits per second

LTM Node Inventory report components

- Node IP address
- Monitor status
- Session state
- Ratio
- Connection limit

LTM Object Activity report components

- Number
- Virtual server name
- Device name
- Connections per second
- Bits per second

SSL TPS Usage report components

- Version (product name, version, and build number)
- Platform
- Serial number
- SSL per core
- Max TPS (maximum number of recorded SSL certificate transactions per second)
- Licensed TPS

Unused LTM Objects report components

- Object type
- Object name

About custom health and activity statistics queries and reports

With Enterprise Manager™ you can collect statistics and view details about the health and activity of the managed devices in your network. You also have the option use this collected data to create your own queries and customized graphs and reports using the details provided in the following sections in conjunction with any MySQL Connector, (available at `http://dev.mysql.com/downloads/connector`).

Overview of statistics types

Enterprise Manager™ stores in its health and performance monitoring database three types of statistics: counter statistics, gauge statistics, and threshold state statistics.

Counter statistics increment periodically to indicate a rate of change. To report the rate of change for a statistic during a specific period of time, the system performs a query for the counter statistics values and the timestamps for the beginning and end of the specified time period. Once the system receives the query response, it calculates and reports the rate of change.

Gauge statistics are absolute values for certain components, such as temperature, fan speed, and current connections. The system does not have to perform a calculation to report the absolute value of a gauge statistic.

A *threshold state statistic* is the current state of a specific statistic value as it relates to its threshold. That is, the threshold state indicates if the statistic value is above, below, or within a specified threshold.

Counter statistic query sample

The following SQL query example retrieves the counter statistic values for the `server_pkts_in` field for a node on the host device, `bigip-central`.

To calculate the rate of change for this example, the system compares the previous value (`perfmon_node_stat p`) and the current value (`perfmon_node_stat c`) in the `perfmon_node_stat` table. With this data, the system calculates the rate of change for the counter statistic using the calculation (V1-V0) / (T1-T0), where V1 is the value of the `server_pkts_in` field at time `c.t`, and V0 is the value of the `server_pkts_in` field at time `p.t`. (The `insert_order` field indicates the previous timestamp and value for that particular node.)

```
SELECT  c.t,
   IFNULL(ABS(ROUND((p.server_pkts_in - c.server_pkts_in) / TIMESTAMPDIFF(SECOND, p.t, c.t))),
 0)
   AS server_pkts_in_per_sec
FROM perfmon_device d, perfmon_device_object o,
perfmon_node_stat c, perfmon_node_stat p
WHERE d.host_name = 'bigip-central'
AND o.perfmon_device_uid = d.uid
AND c.perfmon_device_object_uid = o.uid
AND (p.insert_order = (c.insert_order - 1)
AND p.perfmon_device_object_uid = c.perfmon_device_object_uid)
AND c.t BETWEEN TIMESTAMPADD(MINUTE, -60, NOW()) AND NOW()
AND p.t BETWEEN TIMESTAMPADD(MINUTE, -60, NOW()) AND NOW();
```

Gauge statistic query sample

The following example shows a gauge statistic SQL query that retrieves all values over the past hour for the chassis temperature on the host device, `bigip-central`.

```
SELECT  s.t, s.temperature
      FROM perfmon_device d, perfmon_device_object o,  perfmon_chassis_stat s
      WHERE d.host_name = 'bigip-central'
      AND o.perfmon_device_uid = d.uid
      AND s.perfmon_device_object_uid = o.uid
      AND s.t BETWEEN TIMESTAMPADD(MINUTE, -60, NOW()) AND NOW();
```

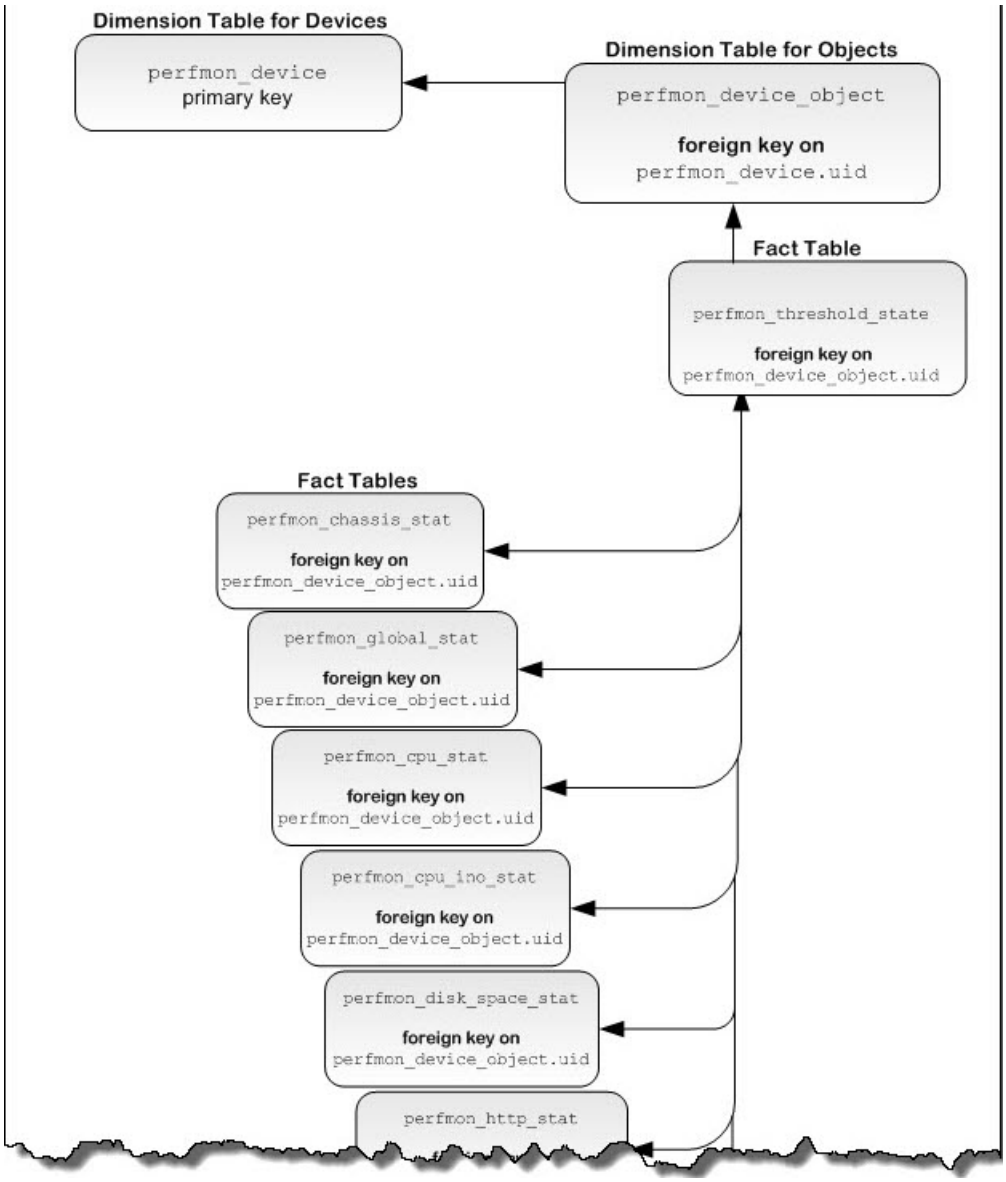
Threshold state statistic query sample

The following SQL query retrieves the current threshold state values for the `perfmon_vip_stat.client_pkts_in` field for all virtual servers associated with managed devices.

```
SELECT
d.host_name, do.name, t.min_threshold, t.max_threshold
FROM
perfmon_threshold_state t,
perfmon_device_object do,
perfmon_device d
WHERE
t.perfmon_device_object_uid = do.uid
AND
t.stat_column_name = 'client_pkts_in'
AND
d.uid = do.perfmon_device_uid
```

About the health and performance monitoring database structure

The Enterprise Manager™ health and performance monitoring database consists of fact tables and dimension tables. The following diagram is an overview of the basic structure of the statistics database.



About dimension tables

Dimension tables contain object-specific details about the statistics for each managed device.

Device identification (perfmon_device)

The `perfmon_device` database table contains details about each managed device.

Field	Type	Null Value Allowed?	Description
`uid`	int unsigned	NO	Primary key
`system_id`	varchar(128)	NO	Device identification

Field	Type	Null Value Allowed?	Description
host_name	varchar(128)	NO	Host name for the device
address	varchar(64)	NO	IP address of the device
boot_location	varchar(16)	NO	Current boot location
product_name	varchar(128)	NO	Name of installed software
product_version	varchar(64)	NO	Version of installed software
product_build_number	varchar(32)	NO	Build number of installed software
ssl_total_tps	int unsigned	YES	Licensed SSL transactions per minute
ssl_per_core	varchar(16)	YES	Indicates if the SSL per core feature is licensed
appliance_sn	varchar(64)	YES	Serial number of the device
platform	varchar(16)	YES	Platform identification number
cpu_count	int	YES	Number of CPU cores on the device

Device object identification (perfmon_device_object)

The perfmon_device_object database table contains identification details about the network objects associated with each managed device.

Field	Type	Null Value Allowed?	Description
uid	int unsigned	NO	Primary key
perfmon_device_uid	int unsigned	NO	Foreign key on perfmon_device.uid
name	varchar(256)	NO	Uniquely identifies this object
perform_object_type	enum	NO	Type of object in the statistics table (global,chassis, cpu,cpu_info, disk_space,udp,tcp, http,clientssl,vip, pool,pool_member,node)

About fact tables

Fact tables contain fields that are specific to the collected statistics type.

Important:

The `partition_number` field is not documented in the following fact tables. Do not reference the `partition_number` field in any custom code that you write, because that field is subject to change.

Chassis statistics (perfmon_chassis_stat)

The `perfmon_chassis_stat` database table contains the temperature statistics of the chassis for each managed device.

Field	Type	Null Value Allowed?	Description	Query Type (if applicable)
`perfmon_device_object_uid`	int unsigned	NO	Used to identify the device and object as the foreign key on `perfmon_device_object.uid`	N/A
`insert_order`	int unsigned	NO	Used to calculate delta values for counter statistics	N/A
`t`	timestamp	NO	Time of data sample	N/A
`temperature`	int unsigned	YES	Temperature of chassis	gauge

CPU statistics (perfmon_cpu_stat)

The `perfmon_cpu_stat` database table contains the temperature and fan speed statistics for each managed device.

Field	Type	Null Value Allowed?	Description	Query Type (if applicable)
`perfmon_device_object_uid`	int unsigned	NO	Used to identify the device and object as the foreign key on `perfmon_device_object.uid`	N/A
`insert_order`	int unsigned	NO	Used to calculate delta values for counter statistics	N/A
`t`	timestamp	NO	Time of data sample	N/A
`fan_speed`	smallint unsigned	YES	Speed of CPU fan	gauge
`temperature`	int unsigned	YES	Temperature of CPU fan	gauge

CPU usage statistics (perfmon_cpu_info_stat)

The `perfmon_cpu_info_stat` database table contains statistics about the CPU usage for each managed device.

Field	Type	Null Value Allowed?	Description	Query Type (if applicable)
`perfmon_device_object_uid`	int unsigned	NO	Used to identify the device and object as the foreign key on `perfmon_device_object.uid`	N/A
`insert_order`	int unsigned	NO	Used to calculate delta values for counter statistics	N/A
`t`	timestamp	NO	Time of data sample	N/A
`cpu_usage_ratio`	smallint unsigned	YES	Ratio of CPU usage to available CPU capacity	gauge

Disk space statistics (perfmon_disk_space_stat)

The `perfmon_disk_space_stat` database table contains details about the disk space for each managed device.

Field	Type	Null Value Allowed?	Description	Query Type (if applicable)
`perfmon_device_object_uid`	int unsigned	NO	Used to identify the device and object as the foreign key on `perfmon_device_object.uid`	N/A
`insert_order`	int unsigned	NO	Used to calculate delta values for counter statistics.	N/A
`t`	timestamp	NO	Time of data sample	N/A
`block_size`	int unsigned	YES	Size of blocks on disk	gauge
`tot_blocks`	int unsigned	YES	Number of blocks on disk	gauge
`free_blocks`	int unsigned	YES	Number of unused blocks on disk	gauge
`block_ratio`	smallint unsigned	YES	Ratio of free blocks to available blocks	gauge
`tot_nodes`	int unsigned	YES	Number of disk nodes	gauge
`free_nodes`	int unsigned	YES	Number of free disk nodes	gauge

GTM pool member statistics (perfmon_gtm_pool_member_stat)

The `perfmon_gtm_pool_member_stat` database table contains performance for each managed Global Traffic Manager™ (GTM™) pool member.

Field	Type	Null Value Allowed?	Description	Query Type (if applicable)
`perfmon_device_object_uid`	int unsigned	NO	Used to identify the device and object as the foreign key on `perfmon_device_object.uid`	N/A
`insert_order`	int unsigned	NO	Used to calculate delta values for counter statistics	N/A
`t`	timestamp	NO	Time of data sample	N/A
`preferred`	int unsigned	YES	Rate of requests per second successfully processed by the configured preferred load balancing method	counter
`alternate`	int unsigned	YES	Rate of requests per second successfully processed by the configured alternate load balancing method	counter
`drop`	int unsigned	YES	Rate of requests per second that were not successfully processed, and were returned to the requesting DNS server	counter
`fallback`	int unsigned	YES	Rate of requests per second that were successfully processed by the configured fall-back load balancing method	counter

GTM pool statistics (perfmon_gtm_pool_stat)

The `perfmon_gtm_pool_stat` database table contains performance statistics for each managed Global Traffic Manager™ (GTM™) pool.

Field	Type	Null Value Allowed?	Description	Query Type (if applicable)
perfmon_device_object_uid	int unsigned	NO	Used to identify the device and object as the foreign key on perfmon_device_object.uid	N/A
insert_order	int unsigned	NO	Used to calculate delta values for counter statistics	N/A
t	timestamp	NO	Time of data sample	N/A
preferred	int unsigned	YES	Rate of requests per second successfully processed by the configured preferred load balancing method	counter
dropped	int unsigned	YES	Rate of requests per second that were not successfully processed, and were returned to the requesting DNS server	counter
fallback	int unsigned	YES	Rate of requests per second that were successfully processed by the configured fall-back load balancing method	counter

GTM virtual server statistics (perfmon_gtm_vs_stat)

The perfmon_gtm_vs_stat database table contains performance and capacity statistics for each managed Global Traffic Manager™ (GTM™) virtual server.

Field	Type	Null Value Allowed?	Description	Query type (if applicable)
perfmon_device_object_uid	int unsigned	NO	Used to identify the device and object as the foreign key on perfmon_device_object.uid	N/A
insert_order	int unsigned	NO	Used to calculate delta values for counter statistics	N/A
t	timestamp	NO	Time of data sample	N/A
cpu	int unsigned	YES	Current amount of CPU used by this GTM virtual server	gauge
mem	int unsigned	YES	Current amount of memory used by this GTM server	gauge
bits_in	int unsigned	YES	Current amount of throughput received, measured in bits per second	gauge
bits_out	int unsigned	YES	Current amount of throughput sent, measured in bits per second	gauge
conn	bigint unsigned	YES	Current number of connections, measured per second	gauge

GTM wide IP statistics (perfmon_gtm_wideip_stat)

This perfmon_gtm_wideip_stat database table contains performance statistics for each managed Global Traffic Manager™ (GTM™) wide IP.

Field	Type	Null value allowed?	Description	Query type (if applicable)
perfmon_device_object_uid	int unsigned	NO	Used to identify the device and object as the foreign key on perfmon_device_object.uid	N/A

Field	Type	Null value allowed?	Description	Query type (if applicable)
insert_order	int unsigned	NO	Used to calculate delta values for counter statistics	N/A
t	timestamp	NO	Time of data sample	N/A
preferred	int unsigned	YES	Rate of requests per second successfully processed by the configured preferred load balancing method	counter
alt	int unsigned	YES	Rate of requests per second successfully processed by the configured alternate load balancing method	counter
dropped	int unsigned	YES	Rate of requests per second that were not successfully processed, and were returned to the requesting DNS server	counter
fallback	int unsigned	YES	Rate of requests per second that were successfully processed by the configured fall-back load balancing method	counter

HTTP traffic statistics (perfmon_http_stat)

The perfmon_http_stat database table contains HTTP-related traffic statistics for each managed device.

Field	Type	Null Value Allowed?	Description	Query Type (if applicable)
perfmon_device_object_uid	int unsigned	NO	Used to identify the device and object as the foreign key on perfmon_device_object.uid	N/A
insert_order	int unsigned	NO	Used to calculate delta values for counter statistics	N/A
t	timestamp	NO	Time of data sample	N/A
http_cookie_persist_inserts	bigint unsigned	YES	Rate of successful attempts to insert HTTP headers for cookie persistence (set-cookie header insertions)	counter
http_resp_2xx_cnt	bigint unsigned	YES	Rate of server-side responses in range of 200 to 206 (successful responses)	counter
http_resp_3xx_cnt	bigint unsigned	YES	Rate of server-side responses in range of 300 to 307 (redirection responses)	counter
http_resp_4xx_cnt	bigint unsigned	YES	Rate of server-side responses in range of 400 to 417 (client errors)	counter
http_resp_5xx_cnt	bigint unsigned	YES	Rate of server-side responses in range of 500 to 505 (server errors)	counter
http_number_reqs	bigint unsigned	YES	Rate of HTTP requests	counter
http_get_reqs	bigint unsigned	YES	Rate of HTTP GET requests	counter
http_post_reqs	bigint unsigned	YES	Rate of HTTP POST requests	counter
http_v9_reqs	bigint unsigned	YES	Rate of version 9 requests	counter
http_v10_reqs	bigint unsigned	YES	Rate of version 10 requests	counter
http_max_keepalive_req	bigint unsigned	YES	Maximum number of requests made in a connection	gauge

Field	Type	Null Value Allowed?	Description	Query Type (if applicable)
http_resp_bucket_1k	bigint unsigned	YES	Rate of responses under 1K	counter
http_resp_bucket_4k	bigint unsigned	YES	Rate of responses between 1K and 4K	counter
http_resp_bucket_16k	bigint unsigned	YES	Rate of responses between 4K and 16K	counter
http_resp_bucket_32k	bigint unsigned	YES	Rate of responses between 16K and 32K	counter
http_resp_bucket_64k	bigint unsigned	YES	This field is deprecated; use larger buckets	counter
http_idle_conn_splices	bigint unsigned	YES	Rate of response bytes before compression is applied	counter
http_idle_conns	bigint unsigned	YES	Rate of idle HTTP connections at the time of query	counter
http_precompress_bytes	bigint unsigned	YES	Rate of response bytes before compression is applied	counter
http_postcompress_bytes	bigint unsigned	YES	Rate of response bytes after compression is applied	counter
http_null_compress_bytes	bigint unsigned	YES	Rate of bytes subjected to NULL compression for license enforcement	counter
http_html_precompress_bytes	bigint unsigned	YES	Rate of bytes for HTML MIME types before compression is applied	counter
http_html_postcompress_bytes	bigint unsigned	YES	Rate of bytes for HTML MIME types after compression is applied	counter
http_css_precompress_bytes	bigint unsigned	YES	Rate of bytes for CSS MIME types before compression is applied	counter
http_css_postcompress_bytes	bigint unsigned	YES	Rate of bytes for CSS MIME types after compression is applied	counter
http_js_precompress_bytes	bigint unsigned	YES	Rate of bytes for JS MIME types before compression is applied	counter
http_js_postcompress_bytes	bigint unsigned	YES	Rate of bytes for JS MIME types after compression is applied	counter
http_xml_precompress_bytes	bigint unsigned	YES	Rate of bytes for XML MIME types before compression is applied	counter
http_xml_postcompress_bytes	bigint unsigned	YES	Rate of bytes for XML MIME types after compression is applied	counter
http_sgml_precompress_bytes	bigint unsigned	YES	Rate of bytes for SGML MIME types before compression is applied	counter
http_sgml_postcompress_bytes	bigint unsigned	YES	Rate of bytes for SGML MIME types after compression is applied	counter
http_plain_precompress_bytes	bigint unsigned	YES	Rate of bytes for plain MIME types before compression is applied	counter
http_plain_postcompress_bytes	bigint unsigned	YES	Rate of bytes for plain MIME types after compression is applied	counter
http_octet_precompress_bytes	bigint unsigned	YES	Rate of bytes for octet MIME types before compression is applied	counter
http_octet_postcompress_bytes	bigint unsigned	YES	Rate of bytes for octet MIME types after compression is applied	counter
http_image_precompress_bytes	bigint unsigned	YES	Rate of bytes for image MIME types before compression is applied	counter
http_image_postcompress_bytes	bigint unsigned	YES	Rate of bytes for image MIME types after compression is applied	counter

Field	Type	Null Value Allowed?	Description	Query Type (if applicable)
http_video_precompress_bytes	bigint unsigned	YES	Rate of bytes for video MIME types before compression is applied	counter
http_video_postcompress_bytes	bigint unsigned	YES	Rate of bytes for video MIME types after compression is applied	counter
http_audio_precompress_bytes	bigint unsigned	YES	Rate of bytes for audio MIME types before compression is applied	counter
http_audio_postcompress_bytes	bigint unsigned	YES	Rate of bytes for audio MIME types after compression is applied	counter
http_other_precompress_bytes	bigint unsigned	YES	Rate of bytes for other MIME types before compression is applied	counter
http_other_postcompress_bytes	bigint unsigned	YES	Rate of bytes for other MIME types after compression is applied	counter
http_ramcache_hits	bigint unsigned	YES	Rate of RAM cache hits	counter
http_ramcache_misses	bigint unsigned	YES	Rate of RAM cache misses	counter
http_ramcache_misses_all	bigint unsigned	YES	Rate of RAM cache misses, including data that could not be cached	counter
http_ramcache_hit_bytes	bigint unsigned	YES	Rate of RAM cache hits, reported in bytes	counter
http_ramcache_miss_bytes	bigint unsigned	YES	Rate of RAM cache misses, excluding data that could not be cached, reported in bytes	counter
http_ramcache_miss_bytes_all	bigint unsigned	YES	Rate of all RAM cache misses, reported in bytes	counter
http_ramcache_size	bigint unsigned	YES	Maximum available RAM cache available, reported in megabytes	gauge
http_ramcache_count	bigint unsigned	YES	Rate of items stored in RAM cache	counter
http_ramcache_evictions	bigint unsigned	YES	Rate of items removed from RAM cache to free memory for new items	counter

Memory usage and connection statistics (perfmon_global_stat)

The perfmon_global_stat database table contains aggregated server-side and client-side statistics about memory usage and connections for each managed device.

Field	Type	Null Value Allowed?	Description	Query Type (if applicable)
perfmon_device_object_uid	int unsigned	NO	Used to identify the device and object as the foreign key on perfmon_device_object.uid	N/A
insert_order	int unsigned	NO	Used to calculate delta values for counter statistics	N/A
t	timestamp	NO	Time of data sample	N/A
client_tot_byte_in	bigint unsigned	YES	Rate of client-side bytes received	counter
client_tot_bytes_out	bigint unsigned	YES	Rate of client-side bytes sent	counter
client_pkts_in	bigint unsigned	YES	Rate of client-side packets received	counter

Field	Type	Null Value Allowed?	Description	Query Type (if applicable)
client_pkts_out	bigint unsigned	YES	Rate of client-side packets sent	counter
client_maxconns	bigint unsigned	YES	Maximum number of client-side connections reported since statistics collection was set or reset for the device	gauge
client_tot_conns	bigint unsigned	YES	Rate of client-side connections per second	counter
client_cur_conns	bigint unsigned	YES	Current number of client-side connections	gauge
server_tot_bytes_in	bigint unsigned	YES	Rate of server-side bytes received	counter
server_tot_bytes_out	bigint unsigned	YES	Rate of server-side bytes sent	counter
server_pkts_in	bigint unsigned	YES	Rate of server-side packets received	counter
server_pkts_out	bigint unsigned	YES	Rate of server-side packets sent	counter
server_maxconns	bigint unsigned	YES	Maximum number of concurrent server-side connections reported since statistics collection was set or reset for the device	gauge
server_cur_conns	bigint unsigned	YES	Current number of active server-side connections	gauge
server_tot_conns	bigint unsigned	YES	Rate of server-side connections	counter
mem	bigint unsigned	YES	Available memory	gauge
mem_used	bigint unsigned	YES	Memory in use	gauge
mem_ratio	smallint unsigned	YES	Ratio of available memory to memory in use	gauge
dropped	bigint unsigned	YES	Rate of dropped packets	counter
err_in	bigint unsigned	YES	Rate of errors received	counter
err_out	bigint unsigned	YES	Rate of errors sent	counter

LTM node statistics (perfmon_node_stat)

The perfmon_node_stat database table contains statistics for traffic and connections to Local Traffic Manager™ (LTM®) node objects for each managed device.

Field	Type	Null value allowed?	Description	Query type (if applicable)
perfmon_device_object_uid	int unsigned	NO	Used to identify the device and object as the foreign key on perfmon_device_object.uid	N/A
insert_order	int unsigned	NO	Used to calculate delta values for counter statistics	N/A
t	timestamp	NO	Time of data sample	N/A

Field	Type	Null value allowed?	Description	Query type (if applicable)
server_tot_bytes_in	bigint unsigned	YES	Total number of server-side bytes received by the specified node address since statistics collection was set or reset for the device	counter
server_tot_bytes_out	bigint unsigned	YES	Rate of server-side bytes sent by the specified node address	counter
server_pkts_in	bigint unsigned	YES	Rate of server-side packets received by the specified node address	counter
server_pkts_out	bigint unsigned	YES	Rate of server-side packets sent by the specified node address	counter
server_maxconns	bigint unsigned	YES	Maximum number of concurrent server-side connections to the specified node address since statistics collection was set or reset for the device	gauge
server_tot_conns	bigint unsigned	YES	Rate of server-side connections to the specified node address	counter
server_cur_conns	bigint unsigned	YES	Current number of active server-side connections to the specified node address	gauge

LTM pool member statistics (perfmon_pool_member_stat)

The perfmon_pool_member_stat database table contains traffic and connection statistics for Local Traffic Manager™ (LTM®) pool members for each managed device.

Field	Type	Null Value Allowed?	Description	Query Type (if applicable)
perfmon_device_object_uid	int unsigned	NO	Used to identify the device and object as the foreign key on perfmon_device_object.uid	N/A
insert_order	int unsigned	NO	Used to calculate delta values for counter statistics	N/A
t	timestamp	NO	Time of data sample	N/A
server_tot_bytes_in	bigint unsigned	YES	Rate of server-side bytes received by the specified pool	counter
server_tot_bytes_out	bigint unsigned	YES	Rater of server-side bytes sent by the specified pool	counter
server_pkts_in	bigint unsigned	YES	Rate of server-side packets received from the specified pool	counter
server_pkts_out	bigint unsigned	YES	Rate of server-side packets sent from the specified pool	counter
server_maxconns	bigint unsigned	YES	Maximum number of concurrent server-side connections to the specified pool reported since statistics collection was set or reset for the device	gauge
server_tot_conns	bigint unsigned	YES	Rate of server-side connections to the specified pool	counter
server_cur_conns	bigint unsigned	YES	Current number of server-side connections to the specified pool	gauge

LTM pool statistics (perfmon_pool_stat)

The `perfmon_pool_stat` database table contains statistics for traffic and connections to Local Traffic Manager™ (LTM®) pools for each managed device.

Field	Type	Null value allowed?	Description	Query type (if applicable)
`perfmon_device_object_uid`	int unsigned	NO	Used to identify the device and object as the foreign key on `perfmon_device_object.uid`	N/A
`insert_order`	int unsigned	NO	Used to calculate delta values for counter statistics	N/A
`t`	timestamp	NO	Time of data sample	N/A
`server_tot_bytes_in`	bigint unsigned	YES	Rate of server-side bytes received by the specified pool	counter
`server_tot_bytes_out`	bigint unsigned	YES	Rate of server-side bytes sent by the specified pool	counter
`server_pkts_in`	bigint unsigned	YES	Rate of server-side packets received from the specified pool	counter
`server_pkts_out`	bigint unsigned	YES	Rate of server-side packets sent from the specified pool	counter
`server_maxconns`	bigint unsigned	YES	Maximum number of server-side connections to the specified pool reported since statistics collection was set or reset for the device	gauge
`server_tot_conns`	bigint unsigned	YES	Rate of server-side connections to the specified pool reported	counter
`server_cur_conns`	bigint unsigned	YES	Current number of active server-side connections to the specified pool	gauge

TCP connection statistics (perfmon_tcp_stat)

The `perfmon_tcp_stat` database table contains TCP connection statistics for each managed device.

Field	Type	Null Value Allowed?	Description	Query Type (if applicable)
`perfmon_device_object_uid`	int unsigned	NO	Used to identify the device and object as the foreign key on `perfmon_device_object.uid`	N/A
`insert_order`	int unsigned	NO	Used to calculate delta values for counter statistics	N/A
`t`	timestamp	NO	Time of data sample	N/A
`open`	int unsigned	YES	Rate of current open TCP connections	counter
`closewait`	int unsigned	YES	Rate of current TCP connections in CLOSE-WAIT/LAST-ACK state	counter
`finwait`	int unsigned	YES	Rate of current connections in FIN-WAIT/CLOSING state	counter
`timewait`	int unsigned	YES	Rate of current connections in TIME-WAIT state	counter
`accept`	bigint unsigned	YES	Rate of TCP connections accepted	counter

Field	Type	Null Value Allowed?	Description	Query Type (if applicable)
acceptfails	bigint unsigned	YES	Rate of TCP connections not accepted	counter
conn	bigint unsigned	YES	Rate of TCP connections established	counter
connfail	bigint unsigned	YES	Rate of TCP connection failures	counter
expires	bigint unsigned	YES	Rate of TCP connections that expired due to idle timeout	counter
abandons	bigint unsigned	YES	Rate of TCP connections abandoned due to retries and Keep-Alive attempts	counter
rxrst	bigint unsigned	YES	Rate of received RST packets	counter
rxbadsum	bigint unsigned	YES	Rate of bad checksum packets	counter
rxbadseg	bigint unsigned	YES	Rate of malformed segments	counter
rxcookie	bigint unsigned	YES	Rate of received SYN-cookies	counter
rxbadcookie	bigint unsigned	YES	Rate of bad SYN-cookies	counter
syncacheover	bigint unsigned	YES	Rate of SYN-cache overflow	counter
txrexmits	bigint unsigned	YES	Rate of retransmitted segments	counter

Threshold state (perfmon_threshold_state)

The `perfmon_threshold_state` database table contains the current threshold state of each managed device.

Field	Type	Null Value Allowed?	Description	Query Type (if applicable)
perfmon_device_object_uid	int unsigned	NO	Used to identify the device and object as the foreign key on `perfmon_device_object.uid`	N/A
stat_column_name	varchar(256)	NO	Identifies the individual statistics to which this threshold applies	threshold
collection interval	int unsigned	NO	Interval at which this statistic is collected	threshold
status	enum	NO	Status of the statistic collection (`enabled`,`disabled`, `profile_change`)	threshold
min_threshold	bigint unsigned	YES	Minimum value of threshold	threshold
threshold_state	enum	NO	State of the threshold range (`BELOW_MIN_THRESHOLD`, `ABOVE_MAX_THRESHOLD`, `WITHIN_THRESHOLD`)	threshold
threshold_exceeded_since	timestamp	YES	Current database has exceeded threshold since this time	threshold
last_alert_fired	timestamp	YES	Time that the last alert was triggered for this out-of-threshold event	threshold

UDP connection statistics (perfmon_udp_stat)

The `perfmon_udp_stat` database table contains UDP connection statistics for each managed device.

Field	Type	Null Value Allowed?	Description	Query Type (if applicable)
`perfmon_device_object_uid`	int unsigned	NO	Used to identify the device and object as the foreign key on `perfmon_device_object.uid`	N/A
`insert_order`	int unsigned	NO	Used to calculate delta values for counter statistics	N/A
`t`	timestamp	NO	Time of data sample	N/A
`open`	int unsigned	YES	Rate of current open UDP connections	counter
`accept`	bigint unsigned	YES	Rte of accepted UDP connections	counter
`acceptfails`	bigint unsigned	YES	Rate of UDP connections that failed because they were not accepted	counter
`conn`	bigint unsigned	YES	Rate of established UDP connections	counter
`connfail`	bigint unsigned	YES	Rate of failed UDP connections	counter
`expires`	bigint unsigned	YES	Rate of expired connections due to idle timeout	counter
`rdxgram`	bigint unsigned	YES	Rate of datagrams received	counter
`rxbaddgram`	bigint unsigned	YES	Rate of malformed datagrams	counter
`rxunreach`	bigint unsigned	YES	Rate of received ICMP messages	counter
`rxnosum`	bigint unsigned	YES	Rate of UDP connections with no checksum	counter
`txdgram`	bigint unsigned	YES	Rate of transmitted datagram packets	counter

LTM virtual server statistics (perfmon_vip_stat)

The `perfmon_vip_stat` database table contains statistics about the connection statistics of Local Traffic Manager™ (LTM®) virtual servers configured for each managed device.

Field	Type	Null Value Allowed?	Description	Query Type (if applicable)
`perfmon_device_object_uid`	int unsigned	NO	Used to identify the device and object as the foreign key on `perfmon_device_object.uid`	N/A
`insert_order`	int unsigned	NO	Used to calculate delta values for counter statistics	N/A
`t`	timestamp	NO	Time of data sample	N/A
`client_tot_byte_in`	bigint unsigned	YES	Rate of client-side bytes received by the specified virtual server	counter
`client_tot_bytes_out`	bigint unsigned	YES	Rate of client-side bytes sent from the specified virtual server	counter

Field	Type	Null Value Allowed?	Description	Query Type (if applicable)
client_pkts_in	bigint unsigned	YES	Rate of client-side packets received by the specified virtual server	counter
client_pkts_out	bigint unsigned	YES	Rate of client-side packets sent from the specified virtual server	counter
client_maxconns	bigint unsigned	YES	Maximum client-side connections to the specified virtual server	gauge
client_tot_conns	bigint unsigned	YES	Rate of client-side connections to the specified virtual server	counter
client_cur_conns	bigint unsigned	YES	Current number of client-side connections to the specified virtual server	gauge

Chapter 6

Managing Application Security Manager Devices

Overview: Application Security Manager device management

You can use Enterprise Manager™ to easily create and deploy security policies, logging profiles, and IP address exception lists to a large set of BIG-IP® Application Security Manager™ devices.

About ASM security policies

At the core of Application Security Manager™ are customized security policies that are tailored to your network environment based on settings that you specify. Instead of logging in to each Application Security Manager device to administer these security policies, you can use Enterprise Manager™ to import, export, and deploy security policies from one central location.

Note: *The method you use to deploy a security policy is dependent on the version of software running on the Application Security Manager devices.*

Importing an ASM security policy

To import a security policy to Enterprise Manager™, you must first create it on the BIG-IP® Application Security Manager™ device.

You can import a security policy to Enterprise Manager to make it available for deployment to other managed Application Security Manager devices or for archiving purposes.

Note: *This procedure is only for BIG-IP Application Security Manger devices running version 11.3.0 or later.*

1. On the Main tab, click **Security** > **Application Security** > **Policies**.
2. Click the **Import** button.
3. For the **Import Method** setting, select an option:
   - Select **Import Security Policy from Device** to choose a device on which you have a security policy
   - Select **Upload Security Policy** to browse to a location where you have saved a security policy.
4. If you are importing the security policy from a device:
   a) Click the name of the device.
   The screen refreshes and displays a list of associated security policies.
   b) Check the select box next to the security policies that you want to import, and click the **Import** button.
   The security policy that you selected displays in the policies list.
5. If you are importing a security policy from a saved file:
   a) Click the **Browse** button.
   b) Browse to the location where you saved the security policy.
   c) Click the **Update** button.
   The security policy that you selected displays in the policies list.

The security policy is now available to deploy to a managed Application Security Manager device.

Deploying an ASM security policy to devices running version 11.3.0 or later

You must first import a security policy to Enterprise Manager™ in order to deploy it.

You can deploy a security policy to one or more managed BIG-IP® Application Security Manager™ devices, without having to log in to each of those devices individually.

Important: *Enterprise Manager must be able to reach the managed device through its management IP address. If Enterprise Manager cannot reach the device's management IP address, deployment fails.*

---

1. On the Main tab, click **Security** > **Application Security** > **Policies**.
2. Click the select button next to the security policy name that you want to deploy, and click the **Deploy** button.
3. Select the check box next to the device name to which you want to deploy this security policy.
4. From the **Deploy Target** list, select the target to which you want to deploy this security policy.

   The target can be a virtual server, policy, or new offline policy. The options displayed depend on the target system's state. If you deploy a new security policy, it overwrites any existing security policy.

The security policy is now available for use on the targeted device.

Exporting an ASM security policy

You must import a security policy from a managed BIG-IP® Application Security Manager™ device to Enterprise Manager™, before you can export it.

You can export a security policy from one web application to use it as a baseline for a new web application. You can also export a security policy to archive it on a remote system before upgrading the system software, or to create a backup copy.

Note: *This procedure is only for BIG-IP Application Security Manger devices running version 11.3.0 or later.*

---

1. On the Main tab, click **Security** > **Application Security** > **Policies**.
2. Click the select button next to the security policy that you want to export, and click the **Export** button. A dialog box opens.
3. Click the **Save** button.
4. Browse to the location that you want to export the security policy to, and click the **Save** button.

The security policy is now available to import to another managed device.

About attack signatures

Attack signatures are the foundation of the BIG-IP® Application Security Manager™ system's negative security logic. *Attack signatures* are rules or patterns that identify attacks, or classes of attacks, on a web application and its components. Enterprise Manager can help you easily manage attack signatures for managed Application Security Manager devices by helping you easily obtain and deploy them to your managed BIG-IP Application Security Manager devices.

Scheduling automatic attack signature file downloads

Attack signature files are applicable only to BIG-IP® Application Security Manager™ devices.

You can create a schedule for Enterprise Manager™ to check for, and download, newly updated attack signature definitions for images stored in the image repository. This feature helps you avoid performing unnecessary and potentially frequent manual checks for updated attack signature files.

Important: *Enterprise Manager checks for updated attack signature files from* `downloads.f5.com`*. For the system to communicate with the F5 servers, you must configure the Enterprise Manager system to use your network DNS server.*

---

1. On the Main tab, click **Enterprise Management** > **Tasks** > **Schedules** > **Attack Signature Updates**.
2. From the **Check for Updates** list, select an option.
   Depending on your selection, the screen refreshes to display the **Start Time** and **Day of the Month/Week** settings.
3. For the **Start Time** setting, select the time of day that you want Enterprise Manager to check for attack signature updates.
4. Depending on the frequency you selected, from the **Day of the Week** or the **Day of the Month** list, select an option.
5. Select the **Automatically Download New Updates** check box.

Enterprise Manager now checks for attack signatures at the specified time interval. If new attack signatures are found, Enterprise Manager downloads the file to its attack signature repository.

Manually checking and downloading updated attack signature files

Attack signature files are applicable only to BIG-IP® Application Security Manager™ devices.

In addition to creating a schedule for automatically checking for attack signature file updates, you can also manually check for and download the most recent attack signature images.

1. On the Main tab, click **Enterprise Management** > **Repository** > **Attack Signature List**.
2. Click the **Check for New Signatures** button.
   The Check for New Signatures screen opens and displays the status of the check for new attack signatures. The screen refreshes at regular intervals as the system checks for available updates for the signature files listed in the Available ASM Attack Signatures section. After the task completes, the system indicates whether an update is available for the signature files in the repository.
3. Click the **Import button.**
   The Import Attack Signature File screen opens.
4. Click the **Browse** button and browse to the location of the Attack Signature file.
5. Click the **Import** button.
   An import status indicator appears, displaying information about the packages as they are downloaded to the image repository.

You can now install the downloaded attack signatures to managed Application Security Manager devices.

By default, Enterprise Manager triggers an alert when a new attack signature is available, however, you must specify the action you want the system to take if the alert is triggered.

Creating an alert for attack signature updates

Before Enterprise Manager can send alerts, you must verify the IP address of your DNS server. If you want Enterprise Manager to send SNMP traps, you must first specify the trap destination.

Create alerts for your devices to monitor specific system events.

1. On the Main tab, click **Enterprise Management** > **Alerts** > **Device Alert List**.
2. Click the **Create** button.
   The New Alert screen opens.
3. In the **Name** field, type a name for the alert.

   Once you create the alert, you cannot change the name.
4. From the **Alert Type** list, select the type of alert that you want to create.
   Depending on the type of alert that you select, the screen may refresh to display additional options, including threshold fields.
5. If the alert type requires a threshold, for the **Condition** setting, specify a threshold value.
6. For the **Action** setting, select the check box next to each action that you want Enterprise Manager to take when the alert is triggered.

   If you select the option, **SNMP trap to remote server**, you must have SNMP configured.
7. If you selected the option to send an email for this alert and you want to specify an address different than the default, clear the **Use default email recipient** check box, and in the **Email Recipient** field, type an email address.

   By default, the system sends an email to the recipient you specified in the Options screen for alerts.
8. If you selected the option to send a message to a remote syslog server and you want to specify an address different than the default, clear the **Use default remote syslog server address** check box and in the **Remote Syslog Server Address** field, type a remote syslog server address.

   By default, the system sends the event to the remote syslog server address you specified in the Options screen for alerts.
9. For the **Devices** or **Devices Lists** setting, in the **Available** box, select one or more devices from the devices or device list and click the Move button to move the selected devices or device list to **Assigned**.
10. Click **Finished**.

Enterprise Manager notifies you if a device meets the criteria for the alert you selected.

Installing an attack signature

An attack signature file must be downloaded (automatically by Enterprise Manager™ or manually) before you can install it on a managed BIG-IP® Application Security Manager™ device. Before installation, verify that the attack signature is the most recent version available.

Important: *For the security policies to work properly, the ASM attack signatures (including custom signatures) must be the same on all systems to which you are deploying the security policies.*

It is important to regularly install updated attack signatures on managed Application Security Manager devices in your network. Enterprise Manager provides you with a simple method of deploying attack signatures to your devices.

1. On the Main tab, click **Enterprise Management** > **Tasks** > **Task List**.
2. Click the **New Task** button.
3. For the **Application Security** setting, select **Install Attack Signatures** and click the **Next** button.

   If the attack signature that you want to install is displayed in the list, you may need to download the attack signature image, or import it to the image repository.
4. From the **Product Version** list, select the software version for which you want to install the attack signature.
   The screen refreshes to display only signatures compatible with the software version you selected.

5. Select the button next to the attack signature the you want to install and click the **Next** button.
6. From the **Device List**, you can select a group of devices to narrow the number of devices displayed.
7. Select the check box next to the Application Security Manager device on which you want to install the attack signature and click the **Next** button.
8. From the **Device Error Behavior** list, select the action you want Enterprise Manager to take in the event that the task fails on one of the devices.
   - **Continue task on remaining devices**
   - **Cancel task on remaining devices**
9. Click the **Next** button.
10. To change the task name, in the **Task Name** field, type a new name.
    This name appears in the task list while the task is running and after the task is finished.
11. Click the **Start Task** button.
    The Task Properties page displays the progress for the task.

When the task completes, the updated attack signature is installed on the selected devices.

About logging profiles for ASM

Enterprise Manager™ manages BIG-IP® Application Security Manager™ logs through logging profiles. A *logging profile* determines where events are logged, and which items (such as which parts of requests, or which type of errors) are logged.

You can create a logging profile that stores logs locally on the managed device, or you can configure the managed device to forward log messages to a remote server.

Creating an ASM logging profile for local storage

A logging profile is applicable only if you are managing BIG-IP® Application Security Manager™ devices.

You create a logging profile to specify the elements of logs that a managed device collects, and to define the storage location. Creating a logging profile allows you to easily apply it to several managed devices, ensuring consistency across your Application Security Manager devices. When locally stored, you can view logs on the managed Application Security Manager device by navigating to the **Security** > **Event Logs** > **Application** > **Requests** screen.

1. On the Main tab, click **Security** > **Application Security** > **Logging Profiles**.
2. Click the **Create** button.
3. In the **Profile Name** field, type a unique identifier for the profile you are creating.
4. For the **Application Security** setting, select the **Enabled** check box.
   The screen refreshes to display additional options.
5. From the **Configuration** list, select **Advanced**.
6. For the **Local Storage** setting, select the **Enabled** check box.
7. To log all requests for a managed device, for the **Guarantee Local Logging** setting, select the **Enabled** check box.

   When enabled, the device logs all requests, even if the logging process slows access to the web application server. When disabled, the device logs all requests as long as the logging process is not competing for system resources. In either case, the managed device does not drop requests.
8. To log specific responses, from the **Response Logging** list, select **For Illegal Requests Only** or **For All Requests**.

9. From the **Storage Filter** list, select **Advanced**.
10. For the **Logic Operation** setting, select the operation that you want the device to use to filter the storage format items that you specified.
    - **OR** prompts the system to log requests based on the traffic elements meeting one or more of the specified criteria.
    - **AND** prompts the system to log requests based on the traffic elements meeting all specified criteria.
11. From the **Request Type** list, select what types of requests to log, **Only Illegal Requests** or **All Requests Types**.
12. To log only traffic from a specific protocol, for the **Protocols** setting, select **Only**, and then select **HTTP** or **HTTPS** from the list.
13. To log traffic only for specific status codes, use the **Response Status Codes** setting:
    a) Select **Only**.
    b) In the **Available Status Codes** list, click each status code that you want to log.
    c) Click the Move button to transfer the selected status code to the **Selected Status Codes** list.
14. To log only traffic from specific HTTP methods, use the **HTTP Methods** setting:
    a) Select **Only**.
    b) In the **Available Methods** list, click each method that you want to log.
    c) Click the Move button to transfer the selected method to the **Selected Methods** list.
15. To log based only on specific strings, use the **Request Containing String** setting:
    a) Select **Search In**.
    b) From the **Search In** list, select an option and type a string in the field.
    The search is case-sensitive.
16. Click the **Finished** button to save this logging profile.

This logging policy is now available to deploy to one or more managed Application Security Manager devices or virtual servers.

Deploying an ASM local storage logging profile to a managed device

You must create a profile before you can deploy it to a BIG-IP® Application Security Manager™ device.

You can deploy a logging profile to a device on which you are remotely storing logs,in order to specify which elements of the traffic are logged.

1. On the Main tab, click **Security** > **Application Security** > **Logging Profiles**.
2. Click the select button next to the profile name you want to deploy and click the **Deploy** button.
3. From the **Deploy to** list, select **Devices**.
4. From the **Device List**, select an option to narrow the list to a specific device.
5. Select the check box next to the device to which you want to deploy this logging profile and click the **Deploy** button.

A window opens displaying the progress of the deployment.

Creating an ASM logging profile for remote storage

A logging profile is applicable only if you are managing BIG-IP® Application Security Manager™ devices.

You create a logging profile to specify the elements of logging. Creating a logging profile allows you to easily apply it to several managed devices, ensuring consistency across your Application Security Manager devices. Storing logs remotely frees room for other processes on the managed device.

1. On the Main tab, click **Security** > **Application Security** > **Logging Profiles**.
2. Click the **Create** button.
3. In the **Profile Name** field, type a unique identifier for the profile you are creating.
4. Select the **Enabled** check box for the **Application Security** setting.
   The screen refreshes to display additional options.
5. From the **Configuration** list, select **Advanced**.
6. To log all requests for a managed device, for **Guarantee Local Logging** setting, select the **Enabled** check box.

   When enabled, the device logs all requests, even if the logging process slows access to the web application server. When disabled, the device logs all requests as long as the logging process is not competing for system resources. In either case, the managed device does not drop requests.
7. For the **Remote Storage** setting, select the **Enabled** check box.
8. To log only specific responses, from the **Response Logging**list, select **For Illegal Requests Only** or **For All Requests**.
9. From the **Remote Storage Type** list, select one of the following:
   - **Remote** - Select this option to store logs on a remote logging server, such as Syslog.
   - **Reporting Server** - Select this option to store logs on a reporting server using a pre-configured storage format. Key/value pairs are used in the log messages.
   - **ArcSight** - Select this option to store logs on a remote logging server using the predefined ArcSight settings for the logs. The log messages are in Common Event Format (CEF).
10. From the **Protocol** list, select the protocol that the remote storage server uses: **TCP**, **TCP-RFC3195**, or **UDP**.
11. For the **Server Address** setting:
    a) In the **IP Address** field, type the IP address for the remote storage server.
    b) From the **Port** list, select the port that the remote storage server uses for traffic and click the **Add** button
12. From the **Facility** list, select the facility category of the logged traffic.
13. For the **Storage Format** setting:
    a) From the list, select **Field-List** to display only pre-defined items in the **Available Items** list. Select **User-Defined** to view pre-defined items in the **Available Items** list and also allow you to type text directly into the **Selected Items** field.
    b) If you selected **Field-List**, in the **CSV with delimiter** field, type symbol to use to separate the objects in the output.

       You may not use the percentage sign (`%`) character. The default delimiter is the comma (`,`) character
    c) From the **Available Items** list, select the items you want to log and click the move button. If you selected **User-Defined** for this setting, you can type a field directly into the **Storage Format** list.
    d) To move an object up or down in the **Selected Items** list, click the item and then click the **Up** or **Down** button.
14. To specify a maximum for how much of the query string the server logs, select the **Length** option and in the **Bytes** field, type a value.
15. If the remote storage server supports TCP protocol, you have the option to change how much of the entry length the server logs by selecting a value from the **Maximum Entry Length** list.

The default length is 1K for remote servers that support the UDP protocol and 2K for remote servers that support the TCP and TCP-RFC3195 protocols.

16. For the **Report Detected Anomalies** setting, select the **Enabled** check box if you want the device to send a report string to the remote device log when a brute force attack, denial of service attack, IP enforcer attack, or web scraping attack starts and ends.
17. From the **Storage Filter** list, select **Advanced**.
18. For the **Logic Operation** setting, select the operation that you want the device to use to filter the storage format items that you specified.
    - **OR** prompts the system to log requests based on the traffic elements meeting one or more of the specified criteria.
    - **AND** prompts the system to log requests based on the traffic elements meeting all specified criteria.
19. From the **Request Type** list, select what types of requests to log, **Only Illegal Requests** or **All Requests Types**.
20. To log only traffic from a specific protocol, for the **Protocols** setting, select **Only**, and then select **HTTP** or **HTTPS** from the list.
21. To log traffic only for specific status codes, use the **Response Status Codes** setting:
    a) Select **Only**.
    b) In the **Available Status Codes** list, click each status code that you want to log.
    c) Click the Move button to transfer the selected status code to the **Selected Status Codes** list.
22. To log only traffic from specific HTTP methods, use the **HTTP Methods** setting:
    a) Select **Only**.
    b) In the **Available Methods** list, click each method that you want to log.
    c) Click the Move button to transfer the selected method to the **Selected Methods** list.
23. To log based only on specific strings, use the **Request Containing String** setting:
    a) Select **Search In**.
    b) From the **Search In** list, select an option and type a string in the field.
    The search is case-sensitive.
24. Click the **Finished** button to save this logging profile.

This logging policy is now available to deploy to one or more managed Application Security Manager devices or virtual servers.

Deploying an ASM remote logging profile to a remote virtual server

You must create a profile before you can deploy it to a BIG-IP® Application Security Manager™ device.

You can deploy a logging profile to a managed device to specify which elements of the traffic are logged.

1. On the Main tab, click **Security** > **Application Security** > **Logging Profiles**.
2. Click the select button next to the profile name you want to deploy, and click the **Deploy** button.
3. From the **Deploy to** list, select **Devices**.
4. From the **Device List**, select an option to narrow the list to a specific device.
5. Select the check box next to the device to which you want to deploy this logging profile and click the **Deploy** button.
   A window opens displaying the progress of the deployment.

This logging profile is now associated with the selected device.

About ASM IP address exception lists

IP address lists contain specified IP addresses that you have deemed as trusted. Managed BIG-IP® Application Security Manager™ devices do not generate Policy Builder learning suggestions for traffic sent from these IP addresses, which reduces unnecessary traffic.

Creating an ASM IP address exception list

An IP address list is applicable only to managed BIG-IP® Application Security Manager™ devices.

IP address exception lists reduce the amount of unnecessary traffic on your managed BIG-IP® Application Security Manager™ devices by defining trusted sites.

1. On the Main tab, click **Security** > **Application Security** > **IP Address Lists**.
2. Click the **Create** button.
3. In the **List Name** field, type a unique name for this list.
4. To import an IP address list:
   a) Click the **Import List** button.
   b) Click the select button next to the device from which you want to import the IP address list, and click the **Next** button.
   c) Select the button next to the security policy from which you want to import the IP address list, and click the **Next** button.
   d) Select the check box next to each IP address exception list you want to add, and click the **Done** button.
5. To add a new IP address exception list and define its properties:
   a) Click the **Add IP Address** button.
   b) In the **IP Address** field, type the IP address you want to add.
   c) In the **Netmask** field, type any associated netmask address.
   d) Specify each setting that you want to enable for this list by selecting its check box.
      Refer to the online help for details about these settings.
   e) In the **Description** field, type an optional description.
   f) Click the **Add** button.

You can now deploy this IP exception list to a security policy.

Deploying an ASM IP address exception list

An IP address list is applicable only to managed BIG-IP® Application Security Manager™ devices. You can deploy an IP address list only after you create one on, or import one to, Enterprise Manager™.

Deploying an IP address list helps reduce traffic on managed Application Security Manager devices.

1. On the Main tab, click **Security** > **Application Security** > **IP Address Lists**.
2. Click the select button next to the IP address list that you want to deploy, and click the **Deploy** button.
3. From the **Deploy to** list, select **Devices**.
4. From the **Device List**, you can select a group of devices to narrow the number of devices displayed.

5. Select the check box next to the device to which you want to deploy this IP address list, and click the **Deploy** button.

   A window opens to display the deployment status.

This IP exception address list is now associated with the selected policy.

Overview: Viewing analytics for multiple ASM devices

You can use Enterprise Manager™ to view reports for managed BIG-IP® Application Security Manager™ devices that are provisioned for Application Visibility and Reporting (AVR).

Analytics reports provide detailed metrics about application performance such as transactions per second, server and client latency, request and response throughput, and sessions. Metrics are provided for applications, virtual servers, pool members, URLs, specific countries, and additional detailed statistics about application traffic running through one or more managed devices. You can view the analytics reports for a single device, view aggregated reports for a group of devices, and create custom lists to view analytics for only specified devices. In this way, Enterprise Manager provides centralized analytics reporting.

Viewing analytics charts and data

Before you can use Enterprise Manager™ to view analytics, you must license it with the Centralized Analytics add-on key. If your web browser is IE8 or earlier, install Adobe® Flash Player on the system where you want to view the analytics. You must also provision the managed BIG-IP® Application Security Manager™ devices for Application Visibility and Reporting (AVR), and associate the analytics profile with one or more virtual servers.

Analytics provide visibility into application behavior, user experience, transactions, and data center resource usage. You can use this information to troubleshoot issues and to increase the efficiency of your network.

1. On the Main tab, click **Statistics** > **Analytics** > **HTTP**.
   The Overview screen opens.
2. For each widget (or area on the screen), click the gear icon, and select **Settings** to adjust what is displayed.

Setting	Description
Devices	Specifies a managed device or a list of managed devices for which you want to display statistics.
View all traffic by	Specifies type of data to view, and provides an optional filter so you can display more information.
Date range	Specifies the time period for which to display statistics (last hour, day, week, month).
Data visualization	Specifies how to format the data (details table, or line, pie, or bar chart).
Available measurements	Specifies up to six measurements to display in Details tables. Line, pie, or bar charts display only the first measurement.

3. From the menu bar, select the type of statistics you want to view.

Select this option	To see these application statistics
Overview	Top statistical information about traffic on your system or managed systems, such as the top virtual servers, top URLs accessed, and top applications. You can customize the information that is displayed.

Select this option	To see these application statistics
Transactions	The HTTP transaction rate (transactions per second) passing through the web applications, and the number of transactions to and from the web applications.
Latency > Server Latency	The number of milliseconds it takes from the time a request arrives at the virtual server until a response arrives at the virtual server.
Latency > Page Load Time	The number of milliseconds it takes for a web page to fully load on a client browser, from the time the user clicks a link or enters a web address until the web page displays in its entirety.
Throughput > Request Throughput	HTTP request throughput in bits per second.
Throughput > Response Throughput	HTTP response throughput in bits per second.
Sessions > New Sessions	The number of transactions that open new sessions, in sessions per second.
Sessions > Concurrent Sessions	The total number of open and active sessions at a given time, until they time out.

The charts display information based on the settings you enabled in the Analytics profile.

4. To specify the devices for which to display application statistics, from the **Device(s)** list, select an option.
   - For multiple devices, select **Device list** and then select the name of a device list. ***All Devices**, provided by default, displays statistics for all managed devices for which AVR is provisioned.
   - For one device, select **Device** and then select the name of the device.

   Tip: *You also have the option to create a custom list of devices by clicking* ***Enterprise Management*** *>* ***Custom Lists*** *and on the Custom Lists screen, clicking* ***Create List****.*

   ---

5. From the **View By** list, select the specific network object type for which you want to display statistics.
   You can also click **Expand Advanced Filters** to filter the information that displays.
6. To focus on specific information, click the chart or the details.
   The system refreshes the charts and displays specific information about the item.

Index

A

B

C

D

E

F

G

H

I

L

M

N

O

P

Q

R

S

T

U