LineRate

Administrator's Guide

Overview

This guide provides additional information for F5$^{®}$ LineRate$^{®}$ administrators, beyond that available in the reference guides.

The content is a work in progress. Only completed content is available, but we will be adding more periodically.

Contents

The guide contains the following sections:

- About This Adminstrator's Guide
- Managing SSL
- Monitoring LineRate

About This Adminstrator's Guide

Overview

This About page contains general information about this guide, including the audience, typographic conventions, and how to search the content.

This guide is a work in progress. Only completed content is available, but we will be adding more periodically.

Audience

This guide is intended for experienced network administrators and network architects who understand your organization's existing TCP/IP network and who need to configure load balancing (reverse proxy) or a forward proxy using F5® LineRate®. It provides additional information, beyond the Getting Started Guide and the reference guides.

Conventions

This guide uses the following symbols and typographic conventions.

Convention	Definition
`Monospaced bold`	Text in a monospaced bold font represents commands or other text that you type exactly as you see it.
`<angle bracket>`	Text in a monospaced bold font inside angle brackets represents a placeholder that describes what you must type.
`[square brackets]`	Text in a monospaced bold font inside square brackets represents an optional command or option.
Monospaced	Text in a monospaced font represents output or results the system displays.
Bold	Text in bold shows keys to press and items to select or click, such as menu items or buttons.
	Shows the beginning of a procedure.
Caution	Cautions contain critical information about configuring your system or data.
Note	Notes contain important information that may affect how you install or configure your system.
Tip	Tips contain best practices or useful information to help you when configuring your system.
	Shows that the content is for advanced users.

Example IP Addresses

Throughout this guide, we use example IP addresses for both internal (private) and external (public) uses.

For private addresses, we use the IP addresses designated in [RFC 1918](#):
- 10.0.0.0 - 10.255.255.255 (10/8 prefix)
- 172.16.0.0 - 172.31.255.255 (172.16/12 prefix)
- 192.168.0.0 - 192.168.255.255 (192.168/16 prefix)

For public addresses, we use the IP addresses designated for documentation in [RFC 5737](#):
- 192.0.2.0/24 (TEST-NET-1)
- 198.51.100.0/24 (TEST-NET-2)
- 203.0.113.0/24 (TEST-NET-3)

Searching the Guide

The search box at the top-right of each page lets you enter a term or phrase to search for. By default, the system searches all pages in the F5$^{®}$ LineRate$^{®}$ content. Searches are not case sensitive. By default, searches find plurals and other matches from word stems, such as tests, testing, tested, and tester if you search for test.

You can search for a single term such as:

```
interface
```

Or

```
certificate
```

You can also search for an exact phrase surrounded by double quotes such as:

```
"real server"
```

Or

```
"IP address"
```

Relevance Level

By default, the system sorts the search results by relevance. The relevance is determined by a weighting algorithm that takes into consideration the page title, content, tags, and attachments. The relevance is

also affected by the page rating (thumb up or down) and by how often other users select a page to view from similar searches.

Searches can return a large number of results. You can narrow your searches a number of ways by:
- Limiting your search to a specific tree
- Using term modifiers
- Using Boolean operators

Limiting a Search to Specific Tree

If you only want to search one area or tree of a guide, you can limit your search to that tree. For example, if you only want to search the Configure Command tree of the 2.6 Release of the CLI Reference Guide for the term "interface," you can enter your search like this:

```
+(path:087Release_2.6/200CLI_Reference_Guide/Configure_Commands/*) AND interface
```

You can further narrow the search using the term modifiers and Boolean operators (described below):

```
+(path:087Release_2.6/200CLI_Reference_Guide/Configure_Commands/*) AND interface
    AND CARP
```

```
+(path:087Release_2.6/*) AND load AND balancer
```

Note: For a tree-specific search, words in quotes are not treated as a specific phrase. The search does an OR search for any words in quotes, so you may not want to use quotes and use AND instead, as shown in the example above.

A few steps to help with this type of search:
1. Navigate to the tree you want to search.
2. In your browser's address bar, copy the address of the page.
   - You only need the part after the "https://docs.lineratesystems.com/".
3. Using the syntax example above, type in your search and paste in the path of the page you want to search.

Term Modifiers

The search supports modifying query terms to provide a wide range of searching options.

Wildcard Searches

The guides support single- and multiple-character wildcard searches with single terms (not within phrase queries).

To perform a single-character wildcard search, use the ? symbol.

To perform a multiple-character wildcard search, use the * symbol.

The single-character wildcard search looks for terms that match that with the single character replaced. For example, to search for "text" or "test" you can use the search:

```
te?t
```

The multiple-character wildcard search looks for 0 or more characters. For example, to search for test, tests or tester, you can use the search:

```
test*
```

You can also use the wildcard searches in the middle of a term.

```
te*t
```

Note: You cannot use a * or ? symbol as the first character of a search.

Fuzzy Searches

The guide supports fuzzy searches based on the Levenshtein Distance or Edit Distance algorithm. To do a fuzzy, search use the tilde ~ symbol at the end of a single word. Fuzzy searches work for multiple characters. For example, to search for a term similar in spelling to "roam" use the fuzzy search:

```
roam~
```

This search will find terms like foam and roams.

You can add an optional parameter to specify the required similarity. The value is between 0 and 1. With a value closer to 1, only terms with a higher similarity will be matched. For example:

```
roam~0.6
```

The default is 0.5.

Proximity Searches

The guide supports finding words that are within a specific distance from each other. To do a proximity search, use the tilde ~ symbol at the end of a phrase. For example, to search for a "feature" and "standard" within 10 words of each other in a document use the search:

```
"feature standard"~10
```

Boosting a Term

The guide provides the relevance level of matching documents based on the terms found. To boost a term, use the caret ^ symbol with a boost factor (a number) at the end of the term you are searching. The higher the boost factor, the more relevant the term will be.

Boosting allows you to control the relevance of a document by boosting its term. For example, if you are searching for:

    mindtouch search

and you want the term "mindtouch" to be more relevant boost it using the ^ symbol along with the boost factor next to the term. You would type:

    mindtouch^4 search

This will make documents with the term mindtouch appear more relevant. You can also boost phrases as in the example:

    "mindtouch search"^4 "Apache"

By default, the boost factor is 1. Although the boost factor must be positive, it can be less than 1 (e.g. 0.2)

Boolean Operators

Boolean operators allow terms to be combined through logic operators. MindTouch supports AND, +, OR, NOT, and - as Boolean operators.

 Note: Boolean operators must be ALL CAPS**.**

OR

The OR operator is the default conjunction operator. This means that if there is no Boolean operator between two terms, the OR operator is used. The OR operator links two terms and finds a matching document if either of the terms exist in a document. This is equivalent to a union using sets. The symbol || can be used in place of the word OR.

To search for documents that contain either "mindtouch search" or just "mindtouch" use the query:

    "mindtouch search" mindtouch

or

    "mindtouch search" OR mindtouch

AND

The AND operator matches documents where both terms exist anywhere in the text of a single document. This is equivalent to an intersection using sets. You can use the symbol && in place of the word AND.

To search for documents that contain "mindtouch search" and "Advanced" use the query:

```
"mindtouch search" AND "Advanced"
```

+

The + (required operator) requires that the term after the + symbol exist somewhere in a document.

To search for documents that must contain "search" and may contain "advanced," use the query:

```
+search advanced
```

NOT

The NOT operator excludes documents that contain the term after NOT. This is equivalent to a difference using sets. You can use the symbol ! in place of the word NOT.

To search for documents that contain "mindtouch search" but not "Advanced" use the query:

```
"mindtouch search" NOT "Advanced"
```

 Note: The NOT operator cannot be used with just one term. For example, the following search will return no results:
NOT "mindtouch search"

Grouping

The guide supports using parentheses to group clauses to form sub queries. This can be very useful if you want to control the Boolean logic for a query.

To search for either "mindtouch" or "search" and "advanced" use the query:

```
(mindtouch OR search) AND advanced
```

This eliminates any confusion and makes sure you that website must exist and either term mindtouch or search may exist.

Escaping Special Characters

The Guide supports escaping special characters that are part of the query syntax. The current list of special characters is:

+ - && || ! ( ) { } [ ] ^ " ~ * ? : \

To escape these character use the \ before the character. For example, to search for (1+1):2 use the query:

```
\(1\+1\)\:2
```

Legal Notices

Copyright

Trademarks

LineRate and SNMP

Overview

F5® LineRate® provides a rich set of statistics and metrics that can be monitored via CLI, REST API, and SNMP. This article discusses a few key metrics that are likely to be of interest to many customers and how to monitor those via SNMP.

SNMP MIB Files

Supported MIBs for any software release may be found on the F5® LineRate® system in two locations. Log into a F5® LineRate® system and issue the `bash` command to enter the bash shell to view or copy the MIBs. The F5® LineRate® proprietary MIBs are located in /usr/linerate/mibs. The standard supported MIBs are located in /usr/local/share/snmp/mibs. Note that not all MIBs and OIDs present in /usr/local/share/snmp/mibs are fully supported.

SNMP Tools

The command line SNMP examples in this article use the Net SNMP tools, running on a F5® LineRate® system from bash. These tools can be found at http://net-snmp.sourceforge.net/. The Net SNMP tools come installed on all F5® LineRate® systems.

LineRate-specific MIBs

MIB File	Description
LRS-CARP-MIB.mib	MIB for Common Address Redundancy Protocol (CARP).
LRS-FAILOVER-MIB.mib	MIB for general management and notification of failover protection.
LRS-FORWARDPROXY-MIB.mib	MIB for configuration and management of forward proxies used in applications such as load balancing (LRS-LB-MIB).
LRS-LB-MIB.mib	MIB for configuration and management of load balancers.
LRS-LICENSING-MIB.mib	MIB for monitoring and traps for licensing.
LRS-MIB.mib	Top-level infrastructure of LineRate's enterprise MIB tree
LRS-NETSTAT-MIB.mib	Configuration and management of LineRate.
LRS-PROCESS-MIB.mib	MIB for configuration and management of LineRate process used in applications such as load balancing (LRS-LB-MIB).
LRS-PRODUCTS-MIB.mib	LineRate Systems product identifiers.
LRS-PROXY-EVENTS-MIB.mib	MIB for system health events.
LRS-REALSERVER-MIB.mib	MIB for configuration and management of real servers used in applications such as load balancing (LRS-LB-MIB).
LRS-SCRIPTING-MIB.mib	MIB for configuration and management of scripts used in applications such as load balancing (LRS-LB-MIB).
LRS-TC.mib	Textual conventions used in the LineRate enterprise MIB.
LRS-VIRTUALSERVER-MIB.mib	MIB for configuration and management of virtual servers used in applications such as load balancing (LRS-LB-MIB).

Enabling SNMP

The following example configuration enables SNMP on all interfaces on the F5® LineRate® system. For best security practice, adjust the configuration below to only enable SNMP on trusted management interface IPs.

```
snmp-server
    enable udpv4 all
    community "mycommunity"
```

MIB OIDs

An SNMP MIB OID can be specified in multiple ways. For example, the lrsAppMgmt OID can be represented the following ways.

Numerically:

```
[admin@host-108a ~]$ snmptranslate -On -IR -M+/usr/linerate/mibs -m ALL lrsAppMgmt

.1.3.6.1.4.1.33661.2.2
```

Symbolically:

```
[admin@host-108a ~]$ snmptranslate -Onf -IR -M+/usr/linerate/mibs -m ALL lrsAppMgmt

.iso.org.dod.internet.private.enterprises.linerate.lrsMgmt.lrsAppMgmt
```

Abbreviated symbolic:

```
[admin@host-108a ~]$ snmptranslate -IR -M+/usr/linerate/mibs -m ALL lrsAppMgmt

LRS-MIB::lrsAppMgmt
```

SNMP tables indexed by object name

Some SNMP tables in the F5® LineRate® MIBs are indexed by the object name string. For example, you can retrieve statistics and information specific to virtual IP "vip1" by looking at its table entries in LRS-LB-MIB. The table is indexed by the name of the object, represented as an explicit string length, followed by the ASCII values of each character in the name. The Net SNMP commands are able to translate string table indexes into OIDs for you. Note that the double quote character is a special character for the bash shell and must be escaped with a backslash when working with the Net SNMP tools.

Tables for real servers and virtual servers are indexed in this same way.

Retrieving open client connections for "vip1":

```
[testlab@host-7 ~]$ snmpget -v2c -c mycommunity -M+/usr/linerate/mibs -m ALL localhost
    LRS-LB-MIB::lrsVipConnClientOpen.\"vip1\"

LRS-LB-MIB::lrsVipConnClientOpen."vip1" = Gauge32: 0
```

Translating just the index portion for the open client connections for "vip1" to a numeric OID:

```
[testlab@host-7 ~]$ snmptranslate -Ob -IR -M+/usr/linerate/mibs -m ALL LRS-LB-
    MIB::lrsVipConnClientOpen.\"vip1\"

LRS-LB-MIB::lrsVipConnClientOpen.4.118.105.112.49
```

Translating to fully numeric OID:

```
[testlab@host-7 ~]$ snmptranslate -On -IR -M+/usr/linerate/mibs -m ALL LRS-LB-
    MIB::lrsVipConnClientOpen.\"vip1\"

.1.3.6.1.4.1.33661.2.2.1.2.1.14.4.118.105.112.49
```

Interesting system and load balancer OIDs

Many statistics in the system are available as a total across all objects in the system and on a per object basis. When applicable, both types of OID are listed. The OID with the capital T in the name (lrsVipT, lrsVST, lrsRST) signifies the total for all objects of that type. For individual named objects, the OID is a table, indexed by object name (see above).

LRS-LB-MIB::lrsVipTConnClientOpen.0 LRS-LB-MIB::lrsVipConnClientOpen."vip1"	Open client connections, in total or for a single named virtual IP.
LRS-LB-MIB::lrsVipTConnClientOpenedPerSec.0 LRS-LB-MIB::lrsVipConnClientOpenedPerSec."vip1"	Rate of client connections opened per second, in total or for a single named virtual IP.
LRS-LB-MIB::lrsVipTHttpClientRequestsPerSec.0 LRS-LB-MIB::lrsVipHttpClientRequestsPerSec."vip1"	Rate of HTTP requests per second, in total or for a single named virtual IP. Valid only for layer 7 HTTP load balancing.

LRS-LB-MIB::lrsVipTBytesRxPerSec.0 LRS-LB-MIB::lrsVipTBytesTxPerSec.0 LRS-LB-MIB::lrsVipBytesRxPerSec."vip1" LRS-LB-MIB::lrsVipBytesTxPerSec."vip1"	Rate of data bytes per second received and transmitted, in total or on a single named virtual IP. Rx refers to bytes received from clients and Tx is bytes transmitted to clients. Note that these rates do not count layer 2-4 headers (e.g. Ethernet, IP, TCP) in the rates.
LRS-VIRTUALSERVER-MIB::lrsVSTHttpServerRequestsPerSec.0 LRS-VIRTUALSERVER-MIB::lrsVSHttpServerRequestsPerSec."vs1"	Rate of HTTP requests per second sent to real servers, in total or on a single named virtual server. Valid only for layer 7 HTTP load balancing.
LRS-VIRTUALSERVER-MIB::lrsVSTHttpClientRequestsPerSec.0 LRS-VIRTUALSERVER-MIB::lrsVSHttpClientRequestsPerSec."vs1"	Rate of incoming HTTP requests per second from clients, in total or on a single named virtual server. Valid only for layer 7 HTTP load balancing.
LRS-VIRTUALSERVER-MIB::lrsVSTTotalQueueSize.0 LRS-VIRTUALSERVER-MIB::lrsVSTotalQueueSize."vs1"	Virtual server queue size, in total or for a single named virtual server. The queue size grows when there is not enough real server capacity to service incoming requests. This can be a good item to monitor to observe real server capacity issues.
LRS-VIRTUALSERVER-MIB::lrsVSTServerL4ConnectionRequestsPerSec.0 LRS-VIRTUALSERVER-MIB::lrsVSServerL4ConnectionRequestsPerSec."vs1"	Rate of layer 4 load balanced connections sent to real servers, in total or on a single named virtual server. Valid only for layer 4 TCP load balancing.
LRS-VIRTUALSERVER-MIB::lrsVSTClientL4ConnectionRequestsPerSec.0 LRS-VIRTUALSERVER-MIB::lrsVSClientL4ConnectionRequestsPerSec."vs1"	Rate of incoming layer 4 load balanced connections from clients, in total or on a single named virtual server. Valid only for layer 4 TCP load balancing.
LRS-REALSERVER-MIB::lrsRSTBytesRxPerSec.0 LRS-REALSERVER-MIB::lrsRSTBytesTxPerSec.0 LRS-REALSERVER-MIB::lrsRSBytesRxPerSec."rs1" LRS-REALSERVER-MIB::lrsRSBytesTxPerSec."rs1"	Rate of data bytes per second received and transmitted, in total or on a single named real server. Rx refers to bytes received from real servers and Tx is bytes transmitted to real servers. Note that these rates do not count layer 2-4 headers (e.g. Ethernet, IP, TCP) in the rates.
LRS-REALSERVER-MIB::lrsRSTConnOpen.0 LRS-REALSERVER-MIB::lrsRSConnOpen."rs1"	Open server connections, in total or for a single named real server.

LRS-REALSERVER-MIB::lrsRSTHttpRequestsPerSec.0 LRS-REALSERVER-MIB::lrsRSHttpRequestsPerSec."rs1"	Rate of HTTP requests per second, in total or for a single named real server. Valid only for layer 7 HTTP load balancing.
LRS-REALSERVER-MIB::lrsRSTConnOpenedPerSec.0 LRS-REALSERVER-MIB::lrsRSConnOpenedPerSec."rs1"	Rate of server connections opened per second, in total or for a single named real server.
UCD-SNMP-MIB::ssCpuIdle.0	Idle CPU as a percentage (0-100).
IF-MIB::ifHCInOctets IF-MIB::ifHCOutOctets	Number of bytes input and output for a particular interface. Note that these are 64-bit counters, unlike the older ifInOctets and ifOutOctets, which are 32-bit counters and are not appropriate for high speed interfaces.

Examples

Walk the load balancing MIB

```
[admin@host-114 ~]$ snmpwalk -v2c -c mycommunity -M+/usr/linerate/mibs -m ALL localhost
    lrsAppMgmt

    LRS-LB-MIB::lrsVipTBytesRx.0 = Counter64: 0
       LRS-LB-MIB::lrsVipTBytesTx.0 = Counter64: 0
       LRS-LB-MIB::lrsVipTBytesRxPerSec.0 = Counter64: 0
       LRS-LB-MIB::lrsVipTBytesTxPerSec.0 = Counter64: 0
       LRS-LB-MIB::lrsVipTConnClientOpened.0 = Counter64: 0
       LRS-LB-MIB::lrsVipTConnClientOpenedPerSec.0 = Counter64: 0
       ...
```

Full output of this command with one virtual IP, one virtual server and one real server configured can be found here.

Monitor total open client connections

Using symbolic name

```
[admin@host-114 ~]$ snmpget -v2c -c mycommunity -M+/usr/linerate/mibs -m ALL localhost
    LRS-LB-MIB::lrsVipTConnClientOpen.0

LRS-LB-MIB::lrsVipTConnClientOpen.0 = Gauge32: 0
```

Same query using numeric OID

```
[admin@host-114 ~]$ snmpget -v2c -c mycommunity -M+/usr/linerate/mibs -m ALL localhost
    .1.3.6.1.4.1.33661.2.2.1.1.14.0

LRS-LB-MIB::lrsVipTConnClientOpen.0 = Gauge32: 0
```

Related Pages

Monitoring LineRate

Monitoring Proxies

Monitoring System Objects

Administrator's Guide

CLI Reference Guide

REST API Reference Guide

Managing SSL

Overview

Secure Sockets Layer (SSL) and Transport Layer Security (TLS) are closely related technologies that provide communication security over an insecure network, such as the Internet. TLS is a standardized protocol, defined by IETF RFCs, and is the successor to the non-standardized SSL protocol. The F5$^®$ LineRate$^®$ software supports both TLS and SSL, for both service type TCP and service type HTTP, but the system and documentation refers to both protocols collectively as "SSL," following the most common industry terminology.

SSL Types Supported in the F5$^®$ LineRate$^®$ Software

The F5$^®$ LineRate$^®$ software supports two types of SSL connections:

- SSL termination—SSL connection from the client to the F5$^®$ LineRate$^®$ load balancer.
- SSL initiation—SSL connection from the F5$^®$ LineRate$^®$ load balancer to the web server.

The diagram below shows the two types of SSL.
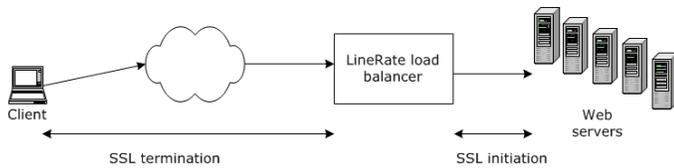
SSL configuration in LineRate

By using the SSL termination feature in F5® LineRate®, you can move the computationally intensive SSL processing off your web servers and onto F5® LineRate®, allowing your web servers to concentrate on performing application tasks. Or, if your application requires greater security on your internal network, you can use SSL initiation together with SSL termination to provide end-to-end SSL security, while still allowing the F5® LineRate® to do full layer 7 load balancing.

Configuring SSL Termination and SSL Initiation

To configure SSL termination:

1. Configure the SSL profile.
   - We recommend using one or more SSL profile bases.
2. Configure certificates and keys.
3. (Optional) Configure chain certificates or certificate bundles.
4. Attach the certificates, keys, and chain certificates to the SSL profile using any of the `attach` commands.
   - You can attach more than one certificate or key to the SSL profile, and the system will determine which are in effect. See Managing Multiple Certificates and Keys.
5. Configure other SSL profile options, as needed.
6. Attach the SSL profile to a virtual IP.

To configure SSL initiation:

1. Configure the SSL profile.
   - We recommend using one or more SSL profile bases.
2. Configure a chain certificate and key.
3. Attach the chain certificates or certificate bundles to the SSL profile using the `attach chain-certificate` command.
4. Configure other SSL profile options, as needed.
   - The following other SSL profile configuration options are applicable to SSL initiation:
     - cipher-list
     - protocol-disable-list
5. Attach the SSL profile to a real server.
6. If using a health monitor with the real server, attached the SSL profile to the health monitor.

Working with Certificate Bundles

You can configure certificate bundles for use as:

- Chain certificate bundle for SSL—Example uses of chain certificate bundles are for performing SSL offload by attaching to a virtual IP or for management access to the system by attaching to the REST server.
- Certificate bundle for a script—Attach a certificate bundle to a script.
- Certificate bundle for an npm registry—Attach a certificate bundle to an npm registry.
- System root certificate bundle—Replace the default system root certificate bundle.

Give each certificate a meaningful name that helps identify the certificate. For example, you might use the domain name or security settings in the name.

SSL Chain Certificate Bundles

The system lets you attach one or more private keys, primary certificates, individual chain certificates, as well as certificate bundles to an SSL profile. Each chain certificate identifies an intermediate Certificate Authority (CA) that can authenticate a primary certificate for the profile.

A certificate bundle is a single file that contains multiple chain certificates concatenated together. The bundle can include related and unrelated chain certificates. The system automatically looks for the chain certificates that correspond to a primary certificate.

Scripts and npm Registries

If you need to customize the certificates, locate the certificates you want to include (create a file or be prepared to copy and paste them inline), configure a new certificate bundle in F5$^{®}$ LineRate$^{®}$, then attach the certificate bundle. The attached certificate bundle acts as the CA root certificate for the script or npm registry.

System Root Certificate Bundle

F5$^{®}$ LineRate$^{®}$ comes with a default system root certificate bundle for general system use. By default, all scripts and npm registries use the default system root certificate bundle.

If you need to customize the system root certificate bundle, locate the certificates you want to include (create a file or be prepared to copy and paste them inline), configure a new certificate bundle in F5$^{®}$ LineRate$^{®}$, then use the `system root-cert-bundle <bundle_name>` command to replace the default system root certificate bundle with your bundle.

When you replace the default system root certificate bundle, F5$^{®}$ LineRate$^{®}$ retains the default bundle and lets you revert back to the default bundle with `no system root-cert-bundle`.

Managing Multiple Certificates and Keys

To ensure that your SSL configuration can support all SSL cipher types for SSL termination, you can attach multiple certificates and keys to a F5® LineRate® SSL profile. Typically, you want to have one certificate/key pair for each cipher type, for example, one pair for RSA ciphers and another pair for ECC ciphers.

How F5® LineRate® Handles Certificates for the Same Cipher Type

You may need two certificate/key pairs for the same cipher type for a short period of time when transitioning to a new certificate/key pair.

Note: Be sure the new certificate and key are have valid start dates when you add them. As shown in the diagrams below, the system will use the certificate with the later expiration date, regardless of the start date.

Only one certificate/key pair for each cipher type will be in effect at a time. In this situation, the system uses the following processes for certificates and keys when you add a new certificate oe key to determine which certificate has precedence.

The diagram below shows how the system handle multiple certificates of the same cipher type.
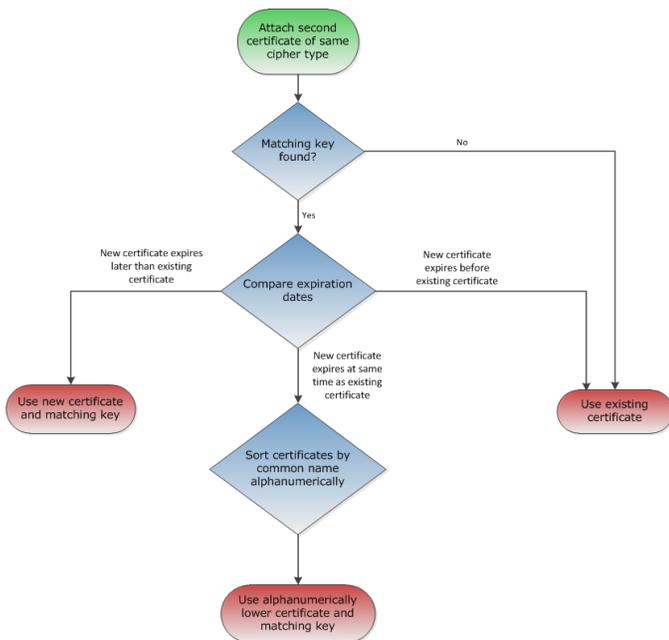
The diagram below shows how the system handle multiple keys of the same cipher type.

Flowchart:

- **Attach key**
- → **Get list of matching certificates. Matching certificate found?**
  - No → **New key not used**
  - Yes → **Get next matching certificate.**
    - → **Compare certificate with existing or last marked certificate**
      - Certificate expires later than existing or last marked certificate → **Mark this certificate for use with new key**
      - Certificate expires before existing or last marked certificate? → **Certificate not used**
      - Certificate expires at same time as existing or last marked certificate → **Sort by common name alphanumerically** → **Mark alphanumerically lower certificate for use with new key**
    - → **All certificates processed?**
      - No → (back to Get next matching certificate)
      - Yes → **If any matching certificate marked, use with new key**

Best Practices

- Configure primary certificates and corresponding keys for each cipher type that clients may use, then attach the configured certificate/key pairs to the SSL profile. For example, for clients that support ECC or RSA ciphers, you may want to configure and attach both RSA and ECC certificates and keys.
- Create one or more SSL profile bases to make configuring SSL profiles more consistent. See base.
- You can configure separate SSL profiles for the same primary certificate, but use different settings in each profile.
- Give each each SSL profile a meaningful name that helps identify it. For example, you might use the domain name or security settings in the name.

FAQ

Below are answers to some common questions related to SSL certificates and keys.

When do certificate/key changes go into effect?

New changes go into effect when the configured certificate/key pair is determined to have the highest precedence of the ones already configured. Any new SSL connections established after this time will use the new certificate/key information. Existing connections will continue to use the certificate/key that was previously in effect.

How should I attach a new certificate/key pair to a virtual IP or real server?

- If the new certificate/key pair is of higher precedence than the one in use on the existing SSL profile, attach it to the existing SSL profile associated with the virtual IP or real server.
- If the new certificate/key pair is of lower precedence than the one in use on the existing SSL profile, create a new SSL profile, attach the certificate/key to the new profile, and attach the new SSL profile to the virtual IP or real server, which replaces the existing SSL profile with the new one.

Is there a limit on the number of certificates or keys that can be attached to an SSL profile?

No. But the recommended guidelines are that users only attach a single certificate/key of a given cipher type at any given time. The only time when it makes sense to have a multiple of these attached is while transitioning from one certificate/key pair to another.

Multiple Certificates Example Configuration

The configuration below, taken from `show run` output, shows an example of a configuration with two RSA certificate/key pairs (called rsa and rsa2) and one ECC certificate/key pair (called ecc) attached to an SSL profile (called test).

```
certificate ecc
 pem-format
-----BEGIN CERTIFICATE-----
MIIBlzCCAT6gAwIBAgIJAJ38j2+cTN4rMAkGByqGSM49BAEwSzELMAkGA1UEBhMC
VVMxETAPBgNVBAgTCENvbG9yYWRvMREwDwYDVQQKEwhMaW5lUmF0ZTEWMBQGA1UE
AxMNbHJvcy10ZXN0LUludDAeFw0xNDEyMTYxMTE4MDBaFw0xNTAxMDUxMTE4MDBa
MEcxCzAJBgNVBAYTAlVTMREwDwYDVQQIEwhDb2xvcmFkbzERMA8GA1UEChMITGlu
ZVJhdGUxEjAQBgNVBAMTCWxyb3MtdGVzdDBZMBMGByqGSM49AgEGCCqGSM49AwEH
A0IABDqeCgA+8VuU/y2m6uF4Xebzo0v/Jn2FD27rEtFGhyLGklUf8C8jc3rz7ig/
0AH2jvXJeZyEmTEBLqyUfolohwujEDAOMAwGA1UdEwQFMAMBAf8wCQYHKoZIzj0E
AQNIADBFAiEAlZBFvZHHu+7de1aFL08Rx93ZLCTYlArqL4iPQGizxh0CIBZ0+hei
03MmNMREqTsvFLQc5BNEAq8O3CIZFhjEPzK3
-----END CERTIFICATE-----
quit
!
certificate rsa
 pem-format
-----BEGIN CERTIFICATE-----
MIICIDCCAYmgAwIBAgIJAJ38j2+cTODTMA0GCSqGSIb3DQEBBQUAMEsxCzAJBgNV
BAYTAlVTMREwDwYDVQQIEwhDb2xvcmFkbzERMA8GA1UEChMITGluZVJhdGUxFjAU
BgNVBAMTDWxyb3MtdGVzdC1JbnQwHhcNMTQxMjE2MTExODAwWhcNMTUwMTA1MTEx
```

ODAwWjBHMQswCQYDVQQGEwJVUzERMA8GA1UECBMIQ29sb3JhZG8xETAPBgNVBAoT
CExpbmVSYXRlMRIwEAYDVQQDEwlscm9zLXRlc3QwgZ8wDQYJKoZIhvcNAQEBBQAD
gY0AMIGJAoGBAKq+j/vj0YlsufuCBOyCYJqDv2MDaag6BpkH0N6z280XjY4Ckahm
n8tEWH/AwODCIkTTYwGnw2BJn6woSLxlbant1U/dNN62B3IAwL+Ze4H76ZJqjofm
K9oTA+KPxs4+MLFKqCSqsaf0IDY+Xqs8QTZCXrfIvV527k91WuFf4eJ3AgMBAAGj
EDAOMAwGA1UdEwQFMAMBAf8wDQYJKoZIhvcNAQEFBQADgYEASgrLLg7Fh7dd1X1W
u2KsUeu19q5m+8YEnRQoElA3cL/AquW8soFk4VjnYj2My1DChR0luCHeW0Uv5b9b
k0uWKjtMkk2b7aIlr5tudDvrgFFths01kdQ1/2zvnNRMWkQMkPhVKwJMm3Pc9cNW
e0b0E1f/RchR9U+HQjtED7pnaO4=
-----END CERTIFICATE-----
quit
!
certificate rsa2
 pem-format
-----BEGIN CERTIFICATE-----
MIIC+zCCAeOgAwIBAgIJALixodCTXfEuMA0GCSqGSIb3DQEBBQUAMBQxEjAQBgNV
BAMMCWxyb3MtdGVzdDAeFw0xNDA4MDcxNjE2MTRaFw0xNTA4MDcxNjE2MTRaMBQx
EjAQBgNVBAMMCWxyb3MtdGVzdDCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoC
ggEBALg6642ij3UdZPTb/DHCRVww+8iDASzcAV+3dDhkL381FZIAF+b4xBkvQFus
Zw1IH4G/FfJJ2IZRYY0+B84ikXE4FvOaVAWA6VP4CjNi+Db+R2iX2HnjRkGRcOd+
VMGy6tE1n/SJcW/fIUDO7/qs9cNKRBtOj2jjoDm4xzR38JWn3XMTsuepxnzmnho+
t/sBeO9MD+FEbYIhVpSiil81Hko0pgQlNGoQSSVb0UxFwl7JJw1fA5ijjrfAylfg
rubLXrgPHsvcK70TSbuORmIysDXcSnAPHcf7Wx87zx4cM0S6kXb5KyTXwUF4Z35S
CkpbsgW/5D80lV/V73Ifq6diNuECAwEAAaNQME4wHQYDVR0OBBYEFObvjG5I1CgU
O93yx8Bxa4sI6fh9MB8GA1UdIwQYMBaAFObvjG5I1CgUO93yx8Bxa4sI6fh9MAwG
A1UdEwQFMAMBAf8wDQYJKoZIhvcNAQEFBQADggEBAIVkk9h/TuEwNAdqlhxSmtZo
s1DostMSJVPJzNWnaPjV6TuquoVps+hKghoADKFXXv1Cjg44zG9Fd3A3uleTE+/4
uUnSpMxu6xCmtG6/GSYGCLvt1zgfah5w6Nq5uEeMboCzXYGxjQEWOcOLVU2xzbPA
dFOfVU4BCcw4Wg9f+sZ4mpYZmgEuXrTjbtPhnGnDudZhbdWl30EghnE6I4qCtGhV
ImAW+MrhHTTqx5NN8lzyTMWkcrLpUJ7C0eb0M7xY2lBqgVHaXcDl7bXIv6lToH0j
4MnKjR3XkWGPP2HphIjZrmDKi2Dt6KVJWTM/4UsvV6GoZAQJui9ZqUQ70hADAvM=
-----END CERTIFICATE-----
quit
!
key ecc
 pem-format
-----BEGIN EC PARAMETERS-----
BggqhkjOPQMBBw==
-----END EC PARAMETERS-----
-----BEGIN EC PRIVATE KEY-----
MHcCAQEEIANFgtofG5wxCgRMKjE/j5RpdCCj2kDMf2JwOxfDJLcEoAoGCCqGSM49
AwEHoUQDQgAEOp4KAD7xW5T/Labq4Xhd5vOjS/8mfYUPbusS0UaHIsaSVR/wLyNz
evPuKD/QAfaO9cl5nISZMQEurJR+iWiHCw==
-----END EC PRIVATE KEY-----
quit
!
key rsa
 pem-format
-----BEGIN RSA PRIVATE KEY-----
MIICXQIBAAKBgQCqvo/749GJbLn7ggTsgmCag79jA2moOgaZB9Des9vNF42OApGo

Zp/LRFh/wMDgwiJE02MBp8NgSZ+sKEi8ZW2p7dVP3TTetgdyAMC/mXuB++mSao6H
5ivaEwPij8bOPjCxSqgkqrGn9CA2Pl6rPEE2Ql63yL1edu5PdVrhX+HidwIDAQAB
AoGANDk29tc2hq7vr6KT+Pbjrz7usc0gaujcjb/bPdKLPw6eKDpW7Mf+xgAwhVqi
Y9xc+Ooi1SXH11KNeO2VWbI4OQpshl3BhrSejRJbF+Z2pfVTBMH1zM0yk+pysIlO
emyUujRviplklM+QeHVhAfbVz4mwdV7RiCWjF2bn5vVlhSECQQDWE3giZJRIBjc1
CTHtSrQeTIkMinAgBYRSosgRewJsHB/BjB06jp21xLmkaGqiOk4EJdCYW21laqba
pLvsdETnAkEAzC6x4oiczXDxoWDOxf6OfrklJSAqylwC2lXnPgfoVo4DYGXfP2mF
oz8sK39PJm/oY9IoUaPklrctaap85FUz8QJBAMBgcp8Fn7Mx0r7YaoOBlGd+A9K/
PY+pJYZVPlFnJ4AbrfXygfmzW8qS5Pj31IvAtYdIrDGeR6rRsuvdCfutaJUCQQCH
X3IrCn5Dq11YrHGLTiG1nRUmjzQvpF9z2L6PHvkI4fEVKZWhWlnzCQBE+oxEpK+D
9yMqNappzpr6UsGpNWBRAkAtqkAEYEspd1R0b+KVFZFur8g4E3h/9bMLRqkRiHYj
7ROHbGhTNBbzu4lOGGy715WOz5/G3aotWZNZwRLIppUk
-----END RSA PRIVATE KEY-----
quit
!
key rsa2
 pem-format
-----BEGIN PRIVATE KEY-----
MIIEvQIBADANBgkqhkiG9w0BAQEFAASCBKcwggSjAgEAAoIBAQC4OuuNoo91HWT0
2/wxwkVcMPvIgwEs3AFft3Q4ZC9/NRWSABfm+MQZL0BbrGcNSB+BvxXySdiGUWGN
PgfOIpFxOBbzmlQFgOlT+AozYvg2/kdol9h540ZBkXDnflTBsurRNZ/0iXFv3yFA
zu/6rPXDSkQbTo9o46A5uMc0d/CVp91zE7LnqcZ85p4aPrf7AXjvTA/hRG2CIVaU
oopfNR5KNKYEJTRqEEklW9FMRcJeyScNXwOYo463wMpX4K7my164Dx7L3Cu9E0m7
jkZiMrA13EpwDx3H+1sfO88eHDNEupF2+Ssk18FBeGd+UgpKW7IFv+Q/NJVf1e9y
H6unYjbhAgMBAAECggEAEiSLSfl2Uzw/0vVPEr9lAT05rndoSDiqUfjJEzyaiNZ7
d1NXB0H8XdaPaffCdkZiA+8DhEbNcfzVtIklT6GL3TB+4iKSn7AgSkqlBoZ6lz/X
XG+HvAkrxA1EpyeDxUePZGb5h6V5bGD272DxtSgPU9oedun3qYaxIr4VsA8XvEUO
8GG7uRZG2n1fliPsBmGltNgRdUW5KQWmcmv1zupGG6TmeD5VSwIffNh5F45EZNFl
h+4UaC0OcPtWGucyZJINNuOAX+8ZLtwJpWtVmqSHb+eQFDyTNc/JARicj68rczOV
h9mZu1LZF6F6JJ6tToCGL4LqjePEnuJED9gt961sIQKBgQDkLIp1UxOwZs9mZDAO
zZNX6DgYX2qb6RDbNgQpXl/VOk8gqDnkO/C5DMhM36rsaKvn/8rviNOolvzgxD65
nyRkY2CmQmn5kdSnBMKYn6ovPZhLL+B1fM3j1WWuyUzBUHnpafP2q63kh+jzv35L
uhlWfTi/RXN5gwJbCF0Ntwu2vQKBgQDOsnp7G8QFZX3eUybFU+smj7G+VgNzPoQW
dUqEbejW6JaAyrZWth6DDB91gkmaa5x6k+aRoc1BrI4A+EBoy2cgDgyBwvtQeZMu
mHPRspUdO+UeRuZAHf+9ORznH0XXPp+qX7ei3WoagSI5CXHacO4pE94/M7t0xDLl
zU+EANzk9QKBgDR1+S+YdkJsoOrNxi7hHSts/Ni9t2k5YOLFvJc2V5pS2baMdyL+
lQ423iaulkHcnwmsSiBguSld7a5P8IwFBvz9zE7tnif/W4E7GvK0YxCRfN5sl5Lr
qvrjKYnSRo97zUvZTHo+ZrDQfsLsGEGY/BJioBV6Bl69vGDpv1tT5qGRAoGATNhD
+vL2rH7wDbDiUCiD2yE/FqFJxRWv692NZ7CpCQUNtzImGhS5QUVHiNt4W8W4NkY4
SVpbQhhR7wBcidldLKisc62221NnqcIaBRMcpvK2mswHHD1K7+GE4lRZFc39dE0D
q7Qfl1z9CTF+t5SWpoTxcpPcFGxA8/ihoFTlyuUCgYEAi3hTykIpc/2arGMg/Hg3
A/dzr+unr+my7eZWKOhEHmzka7sI5VepU+slWzi3ftL6x/Bsx6Smruecc4OosvBJ
QLclgu/RkHQVXAMkhAjTfdf3WfpoO5rTMlKGdWOs50U2hD7m1/9gkzGMuWpxrc7Z
U+nGCxkkyK/9qgAp0YraqTk=
-----END PRIVATE KEY-----
quit
!
ssl profile test
 attach certificate ecc
 attach certificate rsa

```
attach certificate rsa2
attach key ecc
attach key rsa
attach key rsa2
```

Understanding SSL Profile Show Output

The show command for an SSL profile lets you check the profile configuration. Using the example configuration above, the system has determined which of the two RSA certificates to use based on the certificate expiration dates.

A few key things that you can check are:

- In Effect column—Shows which certificates the system is using.
- Cipher List column—Shows which ciphers the system is using, as well as the order in which the system is processing them.
- Active Protocols—Shows which SSL protocols the system is using.
- Ordered Cipher List—Shows the result of the Cipher List, that is, the exact list of ciphers the system is using and the order in which they are used.

```
show ssl profile test
  Configuration:
    Primary Certificates:
      Name                      Origin          Type      Matching Key                    In
    Effect
      rsa2                      set locally     RSA       rsa2
    Yes
      ecc                       set locally     ECC       ecc
     Yes
      rsa                       set locally     RSA       rsa                             No
    (expires sooner)
    Private Keys:
      Name                      Origin          Type      Matching Certificates
      rsa2                      set locally     RSA       rsa2
      ecc                       set locally     ECC       ecc
      rsa                       set locally     RSA       rsa
    Chained Cert Name:
      <none>
    Disabled Protocols List: SSLv2:SSLv3
    Cipher List:              HIGH:!ADH:!SSLv2:!PSK:!ECDH:!kEDH:!SRP:+AES:+3DES default
    ECC Curve List:           prime256v1                                       default
    SSL Session Cache Mode:   auto size                                        default
    SSL Session Cache Size:   10 Mi                                            default
    SSL Session Tickets Mode: enabled                                          default
  Active Protocols: TLSv1:TLSv1.1:TLSv1.2
    Ordered Cipher List:
      Name                      Certificate     Key
      AES256-GCM-SHA384         rsa2            rsa2
      AES256-SHA256             rsa2            rsa2
      AES256-SHA                rsa2            rsa2
```

```
AES128-GCM-SHA256        rsa2              rsa2
AES128-SHA256            rsa2              rsa2
AES128-SHA               rsa2              rsa2
DES-CBC3-SHA             rsa2              rsa2
```

Troubleshooting

If you find that clients are not able to connect using SSL, a few things you can check in F5®️ LineRate®️ include:

- Review the `show run` output to make sure the certificates, keys, SSL profiles, and virtual IPs are configured the way you want them.
- Check the protocol disable list in the `show ssl profile <name>` output to be sure that you are supporting all protocols that clients need.
- Check the SSL profile statistics, shown below, to see if the virtual IP is making connections.

Troubleshooting Performance

If you see performance issues that you think are related to SSL, you can use a show command for each profile to see statistics. You can see if the virtual IP is getting and terminating SSL connections.

```
show ssl profile test statistics

Statistics
    Session Ticket Successes (Termination): 0
    Session Ticket Failures (Termination): 0
    Session Cache Hits (Termination): 0
    Session Cache Misses (Termination): 0
    Cached Session Expired (Termination): 0
    Sessions Reused (Termination): 0
    Sessions negotiated without reuse (Termination): 0
    Sessions Reused (Initiation): 0
    Sessions negotiated without reuse (Initiation): 0
```

Aggregated statistics are available for all SSL profiles using `show ssl statistics`.

If SSL session [tickets](#) or [caching](#) is not enabled, you can use them to improve performance.

Configurations Before Release 2.5

If you attached certificates to SSL profiles in releases before 2.5 and have upgraded to 2.5 or later, the previous attach certificate commands have changed. Before attaching new certificates, you will need to use the `no certificate primary-certificate <cert_name>` and `no private-key`

`<key_name>` commands to remove the existing certificates and keys, then use the new certificate and key commands to re-create them and use the attach command to add the certificates back in.

Related

Getting Started Guide - Configuring SSL

CLI Reference Guide - Certificate Mode Commands

CLI Reference Guide - Key Mode Commands

REST API Reference Guide - certificates or certificateBundles

REST API Reference Guide - keys

Monitoring LineRate

Overview

You can monitor various aspects of the F5® LineRate® system, including system-level (whole "box") information, global proxy statistics, individual proxy statistics, and object-level statistics. Monitoring is available using the F5® LineRate® CLI, REST API, and SNMP MIBs. The syslogs also contain useful information.

The sections that follow describe statistics that you most likely want to monitor and where to find them. Because there are hundreds of available statistics, this guide does not describe every statistic available, but focuses on key statistics to help you monitor and troubleshoot F5® LineRate®.

Brief descriptions of every statistic are available in the SNMP MIBs (SNMP Mode Commands) and the REST API Reference Guide stats section.

Using the CLI

All statistics are available using the CLI. The `show proxy statistics detailed` command produces very lengthy output of all statistics. SNMP and REST are likely more convenient and flexible for ongoing system monitoring. Most of this system monitoring discussion, therefore, focuses on the statistics available using SNMP and REST.

Using F5® LineRate Manager

Some statistics are available for live monitoring using F5® LineRate Manager. You can create line or area charts of the available statistics. However, the statistical data is not saved. For information about creating statistics charts, see Line and Area Charts.

Monitoring the Overall F5® LineRate® System

The table below summarizes the key overall F5® LineRate® system resources that you may want to monitor.

Item	What It Tells You	Where to Find Statistics
Memory and disk	Ensure that the system does not use all available disk space, as that would cause unexpected behavior and lead to a system crash. Large users of disk space are logging, backups, upgrades, and core files (/var/ crash). Ensure that no memory swapping is occurring, as this would mean the system is running out of memory and could cause degraded performance. Following are key functions that affect F5® LineRate® memory usage: • Connection count—Each connection takes memory. • Running a script—Scripts consume memory for each request handled. The amount of memory used varies based on the script design. • SSL session caching. • Use of persistence modes. **Tip:** Using the real server max-connections parameter is a good way to scale the system to handle traffic based on available memory.	**SNMP** Standard SNMP MIB2 MGMT mib OIDs are used to monitor memory and disk usage. • Name: hrStorage • OID: 1.3.6.1.2.1.25.2 • Defined in module: HOST-RESOURCES-MIB • Notable statistics: • hrStorageIndex • hrStorageType • hrStorageDescr • hrStorageAllocationUnits • hrStorageSize • hrStorageUnits • hrStorageAllocationFailures
CPU	The system uses the highest-numbered CPU for management tasks. Monitor this CPU to ensure that the system management does not become overloaded. F5® LineRate® under moderate load reports high CPU usage on the remaining CPUs.	**REST** /status/app/proxy/stats/data/ global/eventLoopTime

Item	What It Tells You	Where to Find Statistics
	Instead of monitoring CPU usage to determine when F5® LineRate® becomes CPU-limited, the proxy event loop time is a more accurate statistic. The event loop time measures the time required for the CPU to process all active connections, averaged across all proxy processes. The event loop time is an input to overall proxy latency, and should be monitored to detect when the system is low on CPU resources. For overall system capacity, monitor the proxy statistics. See Monitoring Proxies and specifically Monitoring Queues.	

Interface and network	Monitor interface bandwidth and errors to ensure ample capacity to handle traffic needs, and that there are no anomalous network conditions causing service degradation.
	
	F5® LineRate® supports standard interface link up and link down SNMP notifications.
		SNMP
		Standard SNMP MIB-2 IF mib OIDs are used to gather interface statistics.
		• Name: ifMib
		• OID: 1.3.6.1.2.1.2
		• Defined in module: IF-MIB
		• Notable stats:
		  • ifInOctets
		  • ifOutOctets
		  • ifInErrors
		  • ifInDiscards
		
		Standard SNMP MIB-2 TCP-MIB mib OIDs are used to gather interface TCP statistics.
		• Name: TCP
		• OID: 1.3.6.1.2.1.6
		• Defined in module: TCP-MIB
		• Notable stats:
		  • tcpActiveOpens
		  • tcpAttemptFails
		  • tcpInErrs
		  • tcpOutRsts

Item	What It Tells You	Where to Find Statistics
		REST /status/system/interface/<name> • ibytes • ierrors • imcasts • packets • iqdrops • obytes • oerrors • omcasts • opackets /status/ip/tcp/statistics

CARP and failover groups	CARP manages the active/standby state of F5® LineRate® systems. The CARP active/standby state changes in response to events such as crashes, lost power, unavailability via the network, or CARP priority changes.
	
	Statistics for CARP and failover groups monitor high availability deployments and are available per interface by CARP virtual host ID and per failover group.
	
	Monitor CARP errors for state changes, which could indicate an unstable or flapping network connectivity between CARP members. F5® LineRate® supports SNMP traps for CARP and failover group state changes.
	
	The CARP state and lastChange nodes show how long the system has been master or standby and tells you when a failover occurred.
		SNMP
		CARP SNMPv2 notification
		• Name: lrsCarpStatusChangeNotification
		• OID: .1.3.6.1.4.1.33661.2.1.4.2.0.1
		• Defined in module: LRS-CARP-MIB
		• Filename: LRS-CARP-MIB.mib
		
		Failover group notification
		• Name: lrsFailoverGroupStatusChangeNotfication
		• OID: .1.3.6.1.4.1.33661.2.1.5.2.0.1
		• Defined in module: LRS-FAILOVER-MIB
		• Filename: LRS-FAILOVER-MIB.mib
		
		REST
		
		/status/system/interface/<name>/carp/<vhid>
		• Notable statistics:
		  • lastChange
		  • state
		
		/status/failover/group/<name>
		• Notable statistics:
		  • lastChange
		  • status

Item	What It Tells You	Where to Find Statistics
Uptime	Monitor the uptime to know when the system was last booted.	**REST** /status/system/uptime
System logs	See Monitoring Errors.	N/A
License	The license expiration lets you know when you need to renew. The system notifies you two days before the expiration.	**REST** /status/app/licensing/feature/base/expiration

Monitoring System Configuration Changes

You may want to monitor system configuration changes, so you can correlate changes in statistics to configuration changes.

Item	What It Tells You	Where to Find Statistics
Configuration changes	Information about when the configuration was last changed and whether the last changes were saved.	**REST** Path: /status/system/config • dirty • lastModifedTime • lastSavedTime • modified
Running diff	Shows the difference between the startup and running configurations. These differnces will not persist across reboots until the running config is copied to the startup config. **Note:** Using this REST node can impact performance, especially for large or complex	/status/system/config/diff

	configurations. Use only as needed.	

Related

[Monitoring Proxies](#)

[Monitoring System Objects](#)

# Monitoring Proxies

Monitoring Proxies

Both reverse and forward proxies have a series of statistics for each configuration object. Statistics aggregate the same way as requests and responses flow through the system, as shown in the diagrams below.

Below, the arrows show the flow of requests through a reverse proxy, with each response following the reverse path of its request. Each object counts stats for all requests and responses that pass thorough it. The dotted boxes show more objects that could be configured, but are omitted for simplicity.

Reverse proxy statistic aggregation
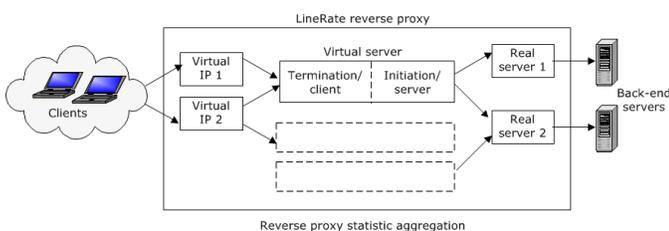
Below, the arrows show the flow of requests through a forward proxy, with each response following the reverse path of its request. Each object counts stats for all requests and responses that pass thorough it.

LineRate forward proxy

Forward proxy statistic aggregation
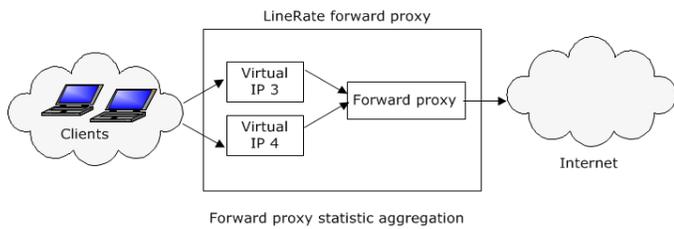
ℹ️   **Note:** If scripts make their own connections via http.request, those connections are not reflected in the statistics for the object shown above. For more information, see Script Statistics.

Statistics are available for each configured object and globally for the whole F5$^®$ LineRate$^®$ system. Use the statistics that meet your monitoring needs.

Monitoring Bandwidth Use

The only bandwidth limit enforced on the F5$^®$ LineRate$^®$ system is specified by the configured license.

For a reverse proxy, the virtual IP has client-side statistics, and the real server has server-side statistics.

For a forward proxy, the virtual IP has client-side statistics, and the forward proxy has server-side statistics.

ℹ️   **Note:** The table below lists only the 1-minute average statistics. Each type of statistic listed also has the average since startup, per second average, and 5-minute average.

The table below summarizes the key F5$^®$ LineRate$^®$ bandwidth statistics that you may want to monitor.

Item	What It Tells You	Where to Find Statistics
Client side	Monitor client-side bandwidth at any or all of the following: • Virtual IP • Global for the entire F5$^®$ LineRate$^®$ system The statistics listed do not include L2 - L4 protocol overhead. They only count TCP payload bytes.	**REST** The available virtual IP statistics are: • connClientBytesRxPerSec1MinAvg • connClientBytesTxPerSec1MinAvg • connClientSslBytesRxPerSec1MinAvg • connClientSslBytesTxPerSec1MinAvg Individual virtual IP statistics are below:

	Notable statistics: • Stats in the connClientBytes family count all bytes received and transmitted on L7, including SSL data. • Stats in the connClientSslBytes family count <u>only</u> received and transmitted SSL data.	• /status/app/proxy/stats/data/ virtualIP/<u><name></u> Aggregate virtual IP statistics are below: • /status/app/proxy/stats/data/ global/<u>virtualIP</u>
Server side	Monitor server-side bandwidth at any or all of the following: • Real server or forward proxy, depending on your configuration • Some global statistics for the entire F5® LineRate® system The statistics listed do not include L2 - L4 protocol overhead. They only count TCP payload bytes. Notable statistics: • Stats in the connClientBytes family count all bytes received and transmitted on L7, including SSL data. • Stats in the connClientSslBytes family count <u>only</u> received and transmitted SSL data.	**REST** The available real server statistics are: • <u>connServerBytesRxPerSec1MinAvg</u> • <u>connServerBytesTxPerSec1MinAvg</u> • <u>connServerSslBytesRxPerSec1MinAvg</u> • <u>connServerSslBytesTxPerSec1MinAvg</u> Individual real server statistics are below: • /status/app/proxy/stats/data/ realServer/<u><name></u> Aggregate real server statistics are below: • /status/app/proxy/stats/data/ global/<u>realServer</u> The available forward proxy statistics are: • <u>connProxyServerBytesRxPerSec1MinAvg</u> • <u>connProxyServerBytesTxPerSec1MinAvg</u> Individual forward proxy statistics are below: • /status/app/proxy/stats/data/ forwardProxy/<u><name></u> Aggregate forward proxy statistics are below: • /status/app/proxy/stats/data/ global/<u>forwardProxy</u>
Interface	See <u>Monitoring the Overall F5® LineRate® System</u>.	N/A

Licensed limits	Statistics related to the licensed limit for bandwidth are available. The F5® LineRate® system applies licensed limits as total throughput of data through the system, not as a limit on any particular interface.	**REST** Available global statistic for throughput rates is: • systemThroughputPerSec1MinAvg Throughput rates are available at: • /status/app/proxy/stats/data/global/ The licensed limit is available from: • /status/app/licensing/ rateLimit/bandwidthRateLimit

Monitoring Latency

F5® LineRate® measures latency at several points in the data path, letting you monitor latency based on your workload and needs.

Note: The table below lists only the 1-minute average statistics. Each type of statistic listed also has instantaneous and 5-minute average statistics.

The table below summarizes the key F5® LineRate® latency statistics that you may want to monitor.

Item	What It Tells You	Where to Find Statistics
Client side	Monitor client-side latency at any or all of the following: • Virtual IP • Virtual server or forward proxy, for aggregated data, depending on your configuration • Global for the entire F5® LineRate® system Client request latency indicates slow network connection. Client response latency could indicate an issue with a real server.	**REST** The available virtual IP statistics are: • httpClientRequestLatency1MinAvg • httpClientRespInitLatency1MinAvg • httpClientRespLatency1MinAvg • httpClientXactionLatency1MinAvg Individual virtual IP statistics are below: • /status/app/proxy/stats/data/ virtualIP/<name> Aggregate virtual IP statistics are below: • /status/app/proxy/stats/data/ global/virtualIP

		The available virtual server statistics are:
		• httpProxyClientRequestLatency1MinAvg
		• httpProxyClientRespInitLatency1MinAvg
		• httpProxyClientRespLatency1MinAvg
		• httpProxyClientXactionLatency1MinAvg
		Individual virtual server statistics are below:
		• /status/app/proxy/stats/data/ virtualServer/<name>
		Aggregate virtual server statistics are below:
		• /status/app/proxy/stats/data/ global/virtualServer
		The available forward proxy statistics are:
		• httpProxyClientRequestLatency1MinAvg
		• httpProxyClientRespInitLatency1MinAvg
		• httpProxyClientRespLatency1MinAvg
		• httpProxyClientXactionLatency1MinAvg
		Individual forward proxy statistics are below:
		• /status/app/proxy/stats/data/ forwardProxy/<name>
		Aggregate forward proxy statistics are below:
		• /status/app/proxy/stats/data/ global/forwardProxy
Server side	Monitor server-side latency at any or all of the following: • Real server and virtual server or forward proxy • Some global for the entire system • For configurations with many real servers and one virtual server, the virtual server gives you aggregated statistics. Server side latency may indicate a network connectivity issue or an issue with a real server processing the request.	**REST** The available real server statistics are: • httpServerRequestInitLatency • httpServerRequestLatency1MinAvg • httpServerRespLatency • httpServerRespLatency1MinAvg • httpServerRespLatency5MinAvg • httpServerXactionLatency • httpServerXactionLatency1MinAvg • httpServerXactionLatency5MinAvg Individual real server statistics are below: • /status/app/proxy/stats/data/ realServer/<name>

Aggregate real server statistics are below:

- /status/app/proxy/stats/data/
global/realServer

The available virtual server statistics are:

- httpProxyServerRequestInitLatency1MinAvg
- httpProxyServerRequestLatency1MinAvg
- httpProxyServerRespLatency1MinAvg
- httpProxyServerXactionLatency1MinAvg

Individual virtual server statistics are below:

- /status/app/proxy/stats/data/
virtualServer/<name>

Aggregate virtual server statistics are below:

- /status/app/proxy/stats/data/
global/virtualServer

The available forward proxy statistics are:

- httpProxyServerRequestInitLatency1MinAvg
- httpProxyServerRequestLatency1MinAvg
- httpProxyServerRespLatency1MinAvg
- httpProxyServerXactionLatency1MinAvg

Individual forward proxy statistics are below:

- /status/app/proxy/stats/data/
forwardProxy/<name>

Aggregate forward proxy statistics are below:

- /status/app/proxy/stats/data/
global/forwardProxy

Monitoring Request and Response Rates

Global TCP connection and HTTP request rate limits are subject to licensed rate limits.

The table below summarizes the key F5® LineRate® HTTP request and response rate statistics that you may want to monitor. For TCP connections, see Monitoring Connections.

Item	What It Tells You	Where to Find Statistics

Client side	Monitor client-side request and response rates at any or all of the following: • Virtual IP • Virtual server or forward proxy, for aggregated data, depending on your configuration • Global for the entire F5® LineRate® system	**REST** The available virtual IP statistics are: • httpClientRequests • httpClientRequestsPerSec • httpClientResp Individual virtual IP statistics are below: • /status/app/proxy/stats/data/ virtualIP/<name> Aggregate virtual IP statistics are below: • /status/app/proxy/stats/data/ global/virtualIP The available virtual server statistics are: • httpProxyClientConnectRequestsPerSec • httpProxyClientRequests • httpProxyClientResp Individual virtual server statistics are below: • /status/app/proxy/stats/data/ virtualServer/<name> Aggregate virtual server statistics are below: • /status/app/proxy/stats/data/ global/virtualServer The available forward proxy statistics are: • httpProxyClientRequests • httpProxyClientRequestsPerSec • httpProxyClientResp Individual forward proxy statistics are below: • /status/app/proxy/stats/data/ forwardProxy/<name> Aggregate forward proxy statistics are below: • /status/app/proxy/stats/data/ global/forwardProxy
Server side	Monitor server-side request and response rates at any or all of the following:	**REST**

	• Real server and virtual server or forward proxy • Some global for the entire F5® LineRate® system • For configurations with many real servers and one virtual server, the virtual server gives you aggregated statistics.	The available real server statistics are: • httpserverConnectRequests • httpServerRequests • httpServerRequestsPerSec • httpServerRespPerSec Individual real server statistics are below: • /status/app/proxy/stats/data/ realServer/<name> Aggregate real server statistics are below: • /status/app/proxy/stats/data/ global/realServer The available virtual server statistics are: • httpProxyServerRequestsPerSec1MinAvg • httpProxyServerRespPerSec1MinAvg Individual virtual server statistics are below: • /status/app/proxy/stats/data/ virtualServer/<name> Aggregate virtual server statistics are below: • /status/app/proxy/stats/data/ global/virtualServer The available forward proxy statistics are: • httpProxyServerRequestsPerSec1MinAvg • httpProxyServerRespPerSec1MinAvg Individual forward proxy statistics are below: • /status/app/proxy/stats/data/ forwardProxy/<name> Aggregate forward proxy statistics are below: • /status/app/proxy/stats/data/ global/forwardProxy
Licensed limits	Statistics related to the licensed limit for HTTP request rate are available.	**REST** Available virtual server statistic is: • licenseProxyRequestRateLimitExceeded

Available below:

- /status/app/proxy/stats/data/ global/virtualServer/

The licensed limit is available from:

- /status/app/licensing/ rateLimit/httpReqRateLimit

Monitoring Connections

Monitoring connection counts tells you if allocated resources are sufficient to handle incoming traffic.

Exceeding connection count limits, global or per object, will cause new connection requests to be dropped (not established).

Connection and request/response rates are not proportional and depend on your configuration, including TCP multiplexing, HTTP keepalive, etc.

Monitoring connection errors indicates a potential issue that could be network related, bad data being received, or point to a back-end system.

Global TCP connection and HTTP request rate limits are subject to licensed rate limits.

A small number of errors might be acceptable under normal operation. However, sudden and continued spikes in connection errors indicate an abnormal condition either on the network or the system.

The table below summarizes the key F5® LineRate® connection statistics that you may want to monitor.

Item	What It Tells You	Where to Find Statistics
Client side	Monitor client-side connections at any or all of the following: • Virtual IP • Virtual server or forward proxy, for aggregated data, depending on your configuration • Global for the entire F5® LineRate® system	**REST** The available virtual IP statistics are: • connAccepted • connClientClosed • connClientErrorSslRequired • connClientFiltered • connClientIdleTimeout • connClientLost • connClientOpen • connClientOpened

- connClientOtherErrors
- connClientReadSize
- connClientRefused
- connClientReset
- connClientTimedOut
- connClientWriteSize
- maxEmbryonicConnsDropped

Individual virtual IP statistics are below:

- /status/app/proxy/stats/data/
  virtualIP/<name>

Aggregate virtual IP statistics are below:

- /status/app/proxy/stats/data/global/virtualIP

The available virtual server statistics are:

- proxyClientL4ConnRequests
- proxyClientL4ConnRequestsPerSec
- proxyClientL4ConnRequestsPerSec1MinAvg
- proxyClientL4ConnRequestsPerSec5MinAvg

Individual virtual server statistics are below:

/status/app/proxy/stats/data/
virtualServer/<name>

Aggregate virtual server statistics are below:

/status/app/proxy/stats/data/
global/virtualServer

The available forward proxy statistics are:

- proxyClientL4ConnRequestsPerSec

Individual forward proxy statistics are below:

- /status/app/proxy/stats/data/
  forwardProxy/<name>

Aggregate forward proxy statistics are below:

- /status/app/proxy/stats/data/
  global/forwardProxy

Server side	Monitor server-side connections at any or all of the following:	**REST** The available real server statistics are:

- Real server and virtual server or forward proxy
- Some global for the entire F5® LineRate® system
- For configurations with many real servers and one virtual server, the virtual server gives you aggregated statistics.

- connServerEarlyEOF
- connServerErrorSslRequired
- connServerIdleTimeout
- connServerInitiated
- connServerLost
- connServerNeedMoreConns
- connServerRefused
- connServerReset

Individual real server statistics are below:

- /status/app/proxy/stats/data/ realServer/<name>

Aggregate real server statistics are below:

- /status/app/proxy/stats/data/ global/realServer

The available virtual server statistics are:
- proxyServerL4ConnRequests
- proxyServerL4ConnRequestsPerSec
- proxyServerL4ConnRequestsPerSec1MinAvg
- proxyServerL4ConnRequestsPerSec5MinAvg
- proxyServerL4ConnSuccessful
- proxyServerL4ConnSuccessfulPerSec
- proxyServerL4ConnSuccessfulPerSec1MinAvg
- proxyServerL4ConnSuccessfulPerSec5MinAvg

Individual virtual server statistics are below:

- /status/app/proxy/stats/data/ virtualServer/<name>

Aggregate virtual server statistics are below:

- /status/app/proxy/stats/data/ global/virtualServer

The available forward proxy statistics are:
- connProxyServerClientClosedEarly
- connProxyserverLost
- connProxyServerOpenedPerSec
- connProxyServerRefused
- connProxyServerIdleTimeout
- proxyServerL4ConnRequestsPerSec
- proxyServerQueueSize1MinAvg
- proxyTotalQueueSize

		Individual forward proxy statistics are below:
		• /status/app/proxy/stats/data/ forwardProxy/<name>
		Aggregate forward proxy statistics are below:
		• /status/app/proxy/stats/data/ global/forwardProxy
Licensed limits	Statistics related to the licensed limit for connections are available.	**REST** The available virtual ip statistics are: • licenseConnectionRateLimitExceeded • licenseConnectionRateLimitExceededPerSec Individual virtual IP statistics are below: • /status/app/proxy/stats/data/ virtualIP/<name> Aggregate virtual IP statistics are below: • /status/app/proxy/stats/data/global/virtualIP The licensed limit is available from: • /status/app/licensing/ rateLimit/tcpConnRateLimit

Monitoring Queues

Monitoring the queues' lengths gives you insight into the load of the system, including back-end servers and client behavior. Work is queued at various stages in the system. The amount of queued work is represented by the queue length.

⚠️ A large queue length can cause increased latency and may cause dropped requests if the queue length reaches the configured limit.

Item	What It Tells You	Where To Find Statistics
Proxy queues	If queue lengths are large, there may not be available real server capacity. If the individual real servers have spare connections or queue space while the virtual server queue length is large, this	The available virtual server statistics are: • proxyRequestMgrDemandExceeded

Item	What It Tells You	Where To Find Statistics
	may indicate that the F5® LineRate® system is limited on some other resource, such as CPU or bandwidth to the clients.	• proxyRequestMgrQueueSize • proxyRequestMgrQueueSize1MinAvg • proxyRequestMgrQueueSize5MinAvg • proxyServerQueueSize • proxyServerQueueSize1MinAvg • proxyServerQueueSize5MinAvg • proxyTotalQueueSize • proxyTotalQueueSize1MinAvg • proxyTotalQueueSize5MinAvg Individual virtual server statistics are below: • /status/app/proxy/stats/data/virtualServer/<name> Aggregate virtual server statistics are below: • /status/app/proxy/stats/data/global/virtualServer
Real Server queues	The maximum real server queue length is (max-in-flight * max conns) and includes any requests in flight. If the real-server queue lengths are large, this may be an indication that the back-end servers are overloaded. Consider adding more back-end servers or increasing real server max-conns or max-inflight. Keep in mind that max-conns should be tuned to the capabilities of the back-end server.	The available real server statistics are: • connServerQueueSize • connServerQueueSize1MinAvg • connServerQueueSize5MinAvg

Monitoring Errors

To monitor errors, refer to the following:
- The other sections in this page for specific errors.
- System logs:

  - /var/log/all.messages

  - /var/log/controller.messages

- Use bash, for example:

  bash "sudo tail -f /var/log/controller.messages"

- For configuring logging options, see Logging Mode Commands.

- Any custom logs you have configured.

Monitoring Capacity

Use the client, server, and global connection data to monitor system capacity. See Monitoring Connections.

Monitoring Request and Response Behavior

HTTP response codes have statistic counters that can be polled for granular picture of HTTP L7 behavior.

The table below summarizes the key F5® LineRate® request and response behavior statistics that you may want to monitor.

Item	What It Tells You	Where to Find Statistics
Client side	Monitor client-side request and response behavior at any or all of the following: • Virtual IP • Virtual server or forward proxy, for aggregated data, depending on your configuration • Global for the entire F5® LineRate® system	**REST** The available virtual IP statistics are: • httpClientConnectRequestsForbidden • httpClientRequestIdleTimeout • httpClientRequestsBad • httpClientRequestsForbidden • httpClientRespIdleTimeout • httpClientRespTimeout • httpInternalRespAttempt5xx The available virtual server statistics are: • httpProxyClientRequestIdleTimeout • httpProxyClientRequestsBad • httpProxyClientRequestsForbidden • httpProxyClientRespIdleTimeout • httpProxyClientRespTimeout Individual virtual server statistics are below:

		• /status/app/proxy/stats/data/ virtualServer/<u>\<name\></u> Aggregate virtual server statistics are below: • /status/app/proxy/stats/data/ global/<u>virtualServer</u> The available forward proxy statistics are: • <u>httpProxyClientConnectRequestsForbidden</u> • <u>httpProxyClientRequestIdleTimeout</u> • <u>httpProxyClientRequestsBad</u> • <u>httpProxyClientRequestsForbidden</u> • <u>httpProxyClientRespIdleTimeout</u> • <u>httpProxyRequestRateLimit503</u> • <u>httpProxyInternalRespAttempt5xx</u> Individual forward proxy statistics are below: • /status/app/proxy/stats/data/ forwardProxy/<u>\<name\></u> Aggregate forward proxy statistics are below: • /status/app/proxy/stats/data/ global/<u>forwardProxy</u>
Server side	Monitor server-side connections at any or all of the following: • Real server and virtual server or forward proxy • Some global for the entire F5® LineRate® system • For configurations with many real servers and one virtual server, the virtual server gives you aggregated statistics.	**REST** The available real server statistics are: • <u>httpServerConnectRequestIdleTimeout</u> • <u>httpServerConnectRequestsAbandoned</u> • <u>httpServerConnectRequestsForbidden</u> • <u>httpServerConnectRespAbandoned</u> • <u>httpServerConnectRespBad</u> • <u>httpServerConnectRespIdleTimeout</u> • <u>httpServerConnectRespNot2xx</u> • <u>httpServerConnectRespTimeout</u> • <u>httpServerErrRxRespBody</u> • <u>httpServerRequestIdleTimeout</u> • <u>httpServerRequestsAbandoned</u> • <u>httpServerRequestsForbidden</u> • <u>httpServerRespAbandoned</u>

- httpServerRespBad
- httpServerRespExtraneous
- httpServerRespIdleTimeout
- httpServerRespLatency
- httpServerRespTimeout

Individual real server statistics are below:

- /status/app/proxy/stats/data/ realServer/<name>

Aggregate real server statistics are below:

- /status/app/proxy/stats/data/ global/realServer

The available virtual server statistics are:

- httpProxyServerConnectRequestIdleTimeout
- httpProxyServerConnectRequestsAbandoned
- httpProxyServerConnectRequestsForbidden
- httpProxyServerConnectRespAbandoned
- httpProxyServerConnectRespBad
- httpProxyServerConnectRespIdleTimeout
- httpProxyServerConnectRespNot2xx
- httpProxyServerConnectRespTimeout
- httpProxyServerErrRxRespBody
- httpProxyServerRequestIdleTimeout
- httpProxyServerRequestsAbandoned
- httpProxyServerRequestsForbidden
- httpProxyServerRespAbandoned
- httpProxyServerRespBad
- httpProxyServerRespExtraneous
- httpProxyServerRespIdleTimeout
- httpProxyServerRespLatency
- httpProxyServerRespTimeout

Individual virtual server statistics are below:

- /status/app/proxy/stats/data/ virtualServer/<name>

Aggregate virtual server statistics are below:

- /status/app/proxy/stats/data/ global/virtualServer

The available forward proxy statistics are:
- httpProxyServerConnectRequestIdleTimeout
- httpProxyServerConnectRequestsAbandoned
- httpProxyServerConnectRequestsForbidden
- httpProxyServerConnectRespAbandoned
- httpProxyServerConnectRespBad
- httpProxyServerConnectRespIdleTimeout
- httpProxyServerConnectRespNot2xx
- httpProxyServerConnectRespTimeout
- httpProxyServerErrRxRespBody
- httpProxyServerRequestIdleTimeout
- httpProxyServerRequestsAbandoned
- httpProxyServerRequestsForbidden
- httpProxyServerRespAbandoned
- httpProxyServerRespBad
- httpProxyServerRespExtraneous
- httpProxyServerRespIdleTimeout
- httpProxyServerRespLatency
- httpProxyServerRespTimeout

Individual forward proxy statistics are below:
- /status/app/proxy/stats/data/ forwardProxy/<name>

Aggregate forward proxy statistics are below:
- /status/app/proxy/stats/data/ global/forwardProxy

Monitoring Scripts

Scripts attach to data path virtual servers and forward proxies and handle requests in between the client side and the server side.

Item	What It Tells You	Where to Find Statistics
Client side	Monitor client-side request and response behavior at any or all of the following: • Virtual server or forward proxy • Script • Global for all scripts on the entire F5® LineRate® system This will show errors for transactions that went through a script, but are caused by a client-side failure: either the client failed, or the script failed to handle the data that the client delivered.	**REST** Individual virtual server statistics relevant to scripting are below: • /status/app/proxy/stats/data/virtualServer/<name> The available virtual server statistics are: • httpProxyRequestScriptDroppedExcept • httpProxyRequestScriptFastPipeFailedC • httpProxyRequestScriptTimeoutExcepti • httpProxyRequestScriptTimeoutExcepti • httpProxyRequestScriptTimeoutExcepti • httpProxyRequestScriptTimeoutExcepti • httpProxyResponseScriptFastPipeFailec Aggregate virtual server statistics are below: • /status/app/proxy/stats/data/global/virtualServer
Server side	Errors for transactions that went through a script, but are caused by a server-side failure: either the server failed, or F5® LineRate® delivered data to the server that it could not handle.	**REST** Individual virtual server statistics relevant to scripting are below: • /status/app/proxy/stats/data/virtualServer/<name> The available virtual server statistics are: • httpProxyRequestScriptFastPipeFailedS • httpProxyResponseScriptFastPipeFailec

Script	Errors and event counts with the script. During normal operation, the counters should show requests going to a script and causing request events to fire, but not causing errors.	**REST** The individual script statistics are below: • /status/app/proxy/stats/ data/script/<name> The available script statistics are: • autoRestarts • requestEvents • requestsRedirected • unrecoverableExceptions

Monitoring SSL

Sustained times of high SSL connection rates could cause service degradation. The virtual IP and real server also have SSL statistics.

The table below summarizes the key F5$^®$ LineRate$^®$ SSL statistics that you may want to monitor.

Item	What It Tells You	Where to Find Statistics
SSL profile	Key statistics to watch for are new initiation and termination connection rates. Most of SSL CPU resource usage is at connection establishment when keys and ciphers are being negotiated. Sustained high SSL connection rates could lead to degraded service. SSL session reuse (session cache or tickets) can significantly improve SSL performance and conserve CPU. See SSL Mode Commands.	**REST** The available SSL profile statistics are: • sessionNewInitPerSec1MinAvg • sessionNewInitPerSec5MinAvg • sessionNewTermPerSec1MinAvg • sessionNewTermPerSec5MinAvg • sessionReuseCacheHitPerSec1MinAvg • sessionReuseCacheHitPerSec5MinAvg • sessionReuseCacheMissPerSec1MinAvg • sessionReuseCacheMissPerSec5MinAvg • sessionReuseExpiredPerSec1MinAvg • sessionReuseExpiredPerSec5MinAvg • sessionReuseTicketHitPerSec1MinAvg • sessionReuseTicketHitPerSec5MinAvg • sessionReuseTicketMissPerSec1MinAvg • sessionReuseTicketMissPerSec5MinAvg • sessionReusedInitPerSec1MinAvg

		• sessionReusedInitPerSec5MinAvg • sessionReusedTermPerSec1MinAvg • sessionReusedTermPerSec5MinAvg Individual SSL profile statistics are below: • /status/ssl/stats/profile/<name> Aggregate SSL profile statistics are below: • /status/ssl/stats/global
SSL Certificates	SSL certificates should be monitored for validity, such as expiration date.	**REST** SSL certificate data is available in: • /status/certificates/ installed/<name>/info • /status/certificateBundles/ installed/<name>/info
Client side	Monitor the virtual IP for client-side SSL statistics.	**REST** The available virtual IP statistics are: • connClientSslAttempt • connClientSslFailed • connClientSslOpened Individual virtual IP statistics are below: • /status/app/proxy/stats/data/ virtualIP/<name> Aggregate virtual IP statistics are below: • /status/app/proxy/stats/data/ global/virtualIP
Server side	Monitor the real server for server (back-end) SSL statistics.	**REST** The available real server statistics are: • connServerErrorSslRequired • connServerSslAttempt • connServerSslBytesRx • connServerSslBytesRxPerSec • connServerSslBytesRxPerSec1MinAvg • connServerSslBytesRxPerSec5MinAvg • connServerSslBytesTx

| | | connServerSslBytesTxPerSec connServerSslBytesTxPerSec1MinAvg connServerSslBytesTxPerSec5MinAvg connServerSslFailed connServerSslOpened Individual real server statistics are below: /status/app/proxy/stats/data/ realServer/<name> Aggregate real server statistics are below: /status/app/proxy/stats/data/ global/realServer |

Related

Monitoring LineRate

Monitoring System Objects

Monitoring System Objects

Overview

Many objects that you can configure in F5$^®$ LineRate$^®$ have statistics you can monitor. Rather than listing all of the statistics, as they are numerous, the sections below provide the REST path to the key object statistics and a link to the documentation. You can explore the statistics listed and determine which ones you want to monitor.

Global Statistics

Global statistics for the whole system are found via REST below /status/app/proxy/stats/data/global.

Below are SNMP OIDs for global statistics.

Object	Name	OID	Defined in module
Virtual IP	lrsVipStatTotal	.1.3.6.1.4.1.33661.2.2.1.1	LRS-LB-MIB
Virtual server	lrsVSStatTotal	.1.3.6.1.4.1.33661.2.2.3.1	LRS-VIRTUALSERVER-MIB
Real server	lrsRealServerStatTotal	.1.3.6.1.4.1.33661.2.2.2.1	LRS-REALSERVER-MIB
Forward proxy	lrsFPStatTotal	.1.3.6.1.4.1.33661.2.2.6.1	LRS-FORWARDPROXY-MIB

Virtual IP Statistics

Virtual IP statistics are found via REST below global (path listed above) and below /status/app/proxy/stats/data/virtualIP/<name>.

Below is the SNMP OID for virtual IP statistics.

Object	Name	OID	Defined in module
Virtual IP (per instance)	lrsVipStatTable	.1.3.6.1.4.1.33661.2.2.1.2	LRS-LB-MIB

Virtual Server Statistics

Virtual server statistics are found vial REST below global (path listed above) and below /status/app/proxy/stats/data/virtualServer/<name>.

Below is the SNMP OID for virtual IP statistics.

Object	Name	OID	Defined in module
Virtual server (per instance)	lrsVSStatTable	.1.3.6.1.4.1.33661.2.2.3.2	LRS-VIRTUALSERVER-MIB

Real Server Statistics

Real server statistics are found via REST below global (above) and below /status/app/proxy/stats/data/realServer/<name>.

Below is the SNMP OID for virtual IP statistics.

Object	Name	OID	Defined in module
Real server (per instance)	lrsRealServerStatTable	.1.3.6.1.4.1.33661.2.2.2.2	LRS-REALSERVER-MIB

Forward Proxy

Forward proxy statistics are found via REST below global (path listed above) and below /status/app/proxy/stats/data/forwardProxy/<name>.

Below is the SNMP OID for virtual IP statistics.

Object	Name	OID	Defined in module
Forward Proxy (per instance)	lrsFPStatTable	.1.3.6.1.4.1.33661.2.2.6.2	LRS-FORWARDPROXY-MIB

Script Statistics

Script statistics are found via REST below global (path listed above) and below /status/app/proxy/stats/ data/script/<name>.

Related

Monitoring LineRate

Monitoring Proxies

Outbound Network Address Translation

1.

Overview

Although F5® LineRate® is not a full-featured network address translation (NAT) device, it can provide some high-scale NAT functionality for outbound traffic when acting as a proxy for this traffic. This document discusses how outbound NAT works with the F5® LineRate®, limitations in the NAT functionality, and some suggested deployment configurations to work around these limitations while still benefitting from F5®'s scalability on outbound connections.

How Outbound NAT Works

F5® LineRate® can be configured as an outbound NAT for select ports by configuring a transparent forward proxy for each port of interest. A sample topology and configuration for performing NAT for all 128.0.0.0/8 and 124.0.0.0/8 destination addresses for TCP traffic on port 80 is show in the figure below.
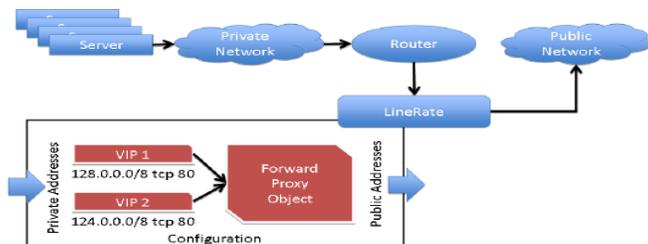
Here, there are two Virtual IPs (VIPs) configured, one for 128.0.0.0/8 port 80 and one for 124.0.0.0/8 port 80, both routing to a single configured forward proxy object on the depicted F5® LineRate®

node. In this configuration, the F5® LineRate® will act as a forward transparent proxy for all incoming port 80 traffic on the designated IP address ranges.

On a 2x6 3.33 GHz Westmere class system with 48 GB of RAM, the F5® LineRate® will terminate approximately 110,000 TCP connections/s with up to 4 million simultaneous connections. Since each proxied connection has both an in-bound and out-bound connection, this amounts to 2,000,000 total simultaneous TCP connections that can be proxied/translated in this fashion.

Limitations

First, since the F5® LineRate® is performing NAT by acting as a TCP proxy, it can only proxy TCP traffic. UDP (for example, DNS) or ICMP (for example, ping) traffic will not be translated. Depending on the configuration of the F5® LineRate®, any such traffic reaching the proxy may be routed to a different interface or will be silently dropped.

Second, each VIP on the F5® LineRate® can only be configured for a single port (but multiple IP addresses). Multiple port NAT is possible by configuring a separate VIP for each port that must be translated. There is currently a limit of 4000 VIPs on any given F5® LineRate® instance.

Third, since the LineRate proxy is not currently a full featured NAT, there are many NAT features - such as address pool configuration, port selection controls, inbound connection support for protocols that make reverse connections (e.g., FTP), and others - that are not be supported at this time.

Deployment Suggestions

Despite F5® LineRate®'s limitations when acting as an outbound NAT, it is still a good solution if a deployment only needs to scale translation for a limited number of outbound ports and has low scale requirements for other ports. In this case, a router that sits between the private nodes requiring outbound NAT and the F5® LineRate® can direct all the high-volume TCP traffic on select ports to the F5® LineRate® using policy-based routing. The routers built-in NAT capability can then be used for low-volume NAT of other traffic such as UDP traffic, ICMP traffic, etc. This deployment, for the addresses above, is depicted in the figure below.
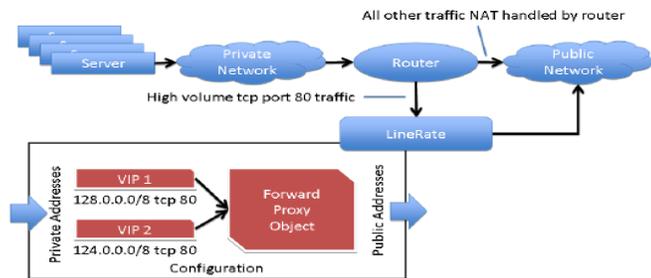
Related Pages

[Virtual IP Mode Commands](#)

[virtualIP](#)

[Forward Proxy Mode Commands](#)

[forwardProxy](#)

[IP Based Protocols](#)

Single-line vs. multi-line configuration for real server and virtual IP

Overview

This article discusses why objects with bases (real server and virtual ip) sometimes show up as a single line in the configuration and sometimes as multiple lines.

Background

F5® LineRate® uses a text-based representation of its configuration to promote understandability of the configuration by humans. However, for very large configurations, the details can easily overwhelm an administrator's ability to understand the configuration. This is why we support bases. Bases allow the administrator to specify common configuration in one place and not repeat unnecessary information.

For objects with bases, the most common case is that the object has only a couple of unique settings, and the rest of the settings are inherited from the object's base. The system understands this common case and generates the shorthand single-line configuration for that object in `show running-config` and in the saved startup-config for this case. This allows an administrator to quickly see which objects are using all the shared settings from the bases (those shown as single-line) versus those that have unique settings applied to that object (those shown as multi-line).

Rules and examples

A real server or virtual IP are shown as a single line in the running-config when the following settings are the only settings applied directly to that object:

- IP address and port
- Base

If any other setting is applied directly to that object, it will appear as multiple lines in the running-config.

In the example below, rs1 is inheriting all its settings (except for base and IP address/port) from base rs_base. However, rs2 has its admin-status set directly on rs2, thus overriding the base. rs1 is online (inherited from rs_base) and rs2 is offline (directly applied to rs2).

```
host-122# show running-config
...
real-server base rs_base
 admin-status online
 max-connections 200
 service http
 !
real-server rs1 ip 10.1.2.3 80 base rs_base
real-server rs2
 ip address 10.1.2.4 80
 base rs_base
 admin-status offline
```

This can be seen more clearly using the **show real-server <name>** command to see where each of the settings on the real server has been obtained from. In the output below, notice that the "Admin Status" line for rs1 shows "inherited from rs_base", but that same line for rs2 shows "set locally".

```
host-122(config-rserver:rs2)# show real-server rs1
Configuration
  Address:               10.1.2.3:80 set locally
  Admin Status:          online      inherited from rs_base
  Max. Connections:      200         inherited from rs_base
  TCP Options:           <none>      default
  SSL Profile:           <none>      default
  Service Type:          http        inherited from rs_base
  Health Monitors:
    <none>
  Max. Request In Flight: 1          default
  Keepalive Timeout:     0 s         default
  Response Timeout:      0 s         default
  Response Idle Timeout: 0 s         default
  Request Idle Timeout:  0 s         default
  Tunnel Idle Timeout:   0 s         default
  Is Proxy:              0           default
Current Status
  Health Status: up (no mon)
host-122(config-rserver:rs2)# show real-server rs2
Configuration
  Address:               10.1.2.4:80 set locally
  Admin Status:          offline     set locally
  Max. Connections:      200         inherited from rs_base
  TCP Options:           <none>      default
  SSL Profile:           <none>      default
  Service Type:          http        inherited from rs_base
  Health Monitors:
    <none>
  Max. Request In Flight: 1          default
  Keepalive Timeout:     0 s         default
  Response Timeout:      0 s         default
  Response Idle Timeout: 0 s         default
  Request Idle Timeout:  0 s         default
  Tunnel Idle Timeout:   0 s         default
  Is Proxy:              0           default
Current Status
  Health Status: up (no mon)
```

Returning an object to single-line output

To return an object to single-line output mode, you must remove all settings that are directly applied to that object, other than base and IP address/port. To remove a setting from an object, use the **no** form of the command. In the example above, rs2 has **admin-status offline** applied directly to rs2. To remove that setting, use **no admin-status offline**. This will remove that setting from rs2, and rs2 will resume inheriting that setting from rs_base. In the output below, note how rs1 and rs2 are now both in single-line output mode and real server rs2 shows that it is inheriting its admin-status from rs_base.

```
host-122(config)# real-server rs2
host-122(config-rserver:rs2)# no admin-status offline
host-122(config-rserver:rs2)# show running-config
...
real-server base rs_base
 admin-status online
 max-connections 200
 service http
!
real-server rs1 ip 10.1.2.3 80 base rs_base
real-server rs2 ip 10.1.2.4 80 base rs_base
...
host-122(config-rserver:rs2)# show real-server rs2
Configuration
  Address:               10.1.2.4:80 set locally
  Admin Status:          online       inherited from rs_base
  Max. Connections:      200          inherited from rs_base
  TCP Options:           <none>       default
  SSL Profile:           <none>       default
  Service Type:          http         inherited from rs_base
  Health Monitors:
    <none>
  Max. Request In Flight: 1           default
  Keepalive Timeout:     0 s          default
  Response Timeout:      0 s          default
  Response Idle Timeout: 0 s          default
  Request Idle Timeout:  0 s          default
  Tunnel Idle Timeout:   0 s          default
  Is Proxy:              0            default
Current Status
  Health Status: up (no mon)
```

Related Pages

Real Server Mode Commands

realServer

Virtual IP Mode Commands

virtualIP