BIG-IP® New Features Guide for version 4.6

MAN-0084-00

Legal Notices

Copyright

F5 Networks, Inc. (F5) believes the information it furnishes to be accurate and reliable. However, F5 assumes no responsibility for the use of this information, nor any infringement of patents or other rights of third parties which may result from its use. No license is granted by implication or otherwise under any patent, copyright, or other intellectual property right of F5 except as specifically described herein. F5 reserves the right to change specifications at any time without notice.

Trademarks

F5, F5 Networks, the F5 logo, BIG-IP, 3-DNS, iControl, Packet Velocity, Internet Control Architecture, IP Application Switch, SYN Check, GLOBAL-SITE, SEE-IT, EDGE-FX, FireGuard, iRules, Control Your World, uRoam, and FirePass are registered trademarks or trademarks of F5 Networks, Inc. in the U.S. and certain other countries. All other trademarks mentioned in this document are the property of their respective owners. F5 Networks' trademarks may not be used in connection with any product or service except as permitted in writing by F5.

Patents

This product protected by U.S. Patent 6,374,300; 6,473,802. Pending U.S. Patent 20020040400. Other patents pending.

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.

Export 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 generates, uses, and may emit radio frequency energy. The equipment has been type tested and found to comply with the limits for a Class A digital device pursuant to Part 15 of FCC rules, which are designed to provide reasonable protection against such radio frequency interference.

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

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

Canadian Regulatory Compliance

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

Standards Compliance

The product conforms to ANSI/UL Std 1950 and Certified to CAN/CSA Std. C22.2 No. 950.

Acknowledgments

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

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

Table of Contents

1

Introduction to this Guide

- What's new in BIG-IP version 4.6
- Using this guide

What’s new in BIG-IP version 4.6

The BIG-IP software version 4.6 release includes a number of new features. These features include enhancements to CRL authentication, SSL proxy re-encryption, and ICMP message handling.

The new features in this release are documented either in this guide or in the release note for BIG-IP software version 4.6. For a complete list of the new features in this release, see the release note.

The new features documented in this guide are:

- **SSL proxy selective encryption**
  SSL proxy server-side re-encryption at the pool level allows you to override the re-encryption option for selected pools. This is useful for configurations that include a local pool that does not require server-side re-encryption and a remote pool that requires server-side re-encryption. For more information, see Chapter 2, *SSL Proxy Selective Re-encryption*.

- **Node counting**
  This release includes the **active_nodes** function which indicates how many nodes are available in a pool. The **active_nodes** function is useful for configuring rules that send traffic to a particular pool based on how many nodes are available in that pool. For more information, see Chapter 3, *Node Counting Rule Function*.

- **CRL authentication enhancements**
  This release includes enhancements to CRL functionality including the addition of CRL management using distribution points and a configurable update interval that refreshes CRLs at a specified interval. For more information, see Chapter 4, *CRL Authentication Enhancements*.

Using this guide

Before using this guide, it is helpful to understand how the guide relates to other BIG-IP documentation. It is also helpful to understand the stylistic conventions that appear throughout the text.

Scope of this guide

This guide documents only those new features that are included in the BIG-IP version 4.6 release. You should therefore use this guide in conjunction with the complete set of product documentation that applies to the BIG-IP version 4.6 release.

The BIG-IP version 4.6 documentation set comprises these documents:

- **Platform Guide version 4.5**
  This guide includes information about the BIG-IP unit. It also contains important environmental warnings.
- **BIG-IP Solutions Guide version 4.5**
  This guide provides examples of common load balancing solutions.
- **BIG-IP Reference Guide version 4.5**
  This guide provides detailed configuration information for the BIG-IP system. It also provides syntax information for **bigpipe** commands, other command line utilities, configuration files, system utilities, and monitoring and administration information.
- **Link Controller Solutions Guide version 4.5**
  This guide provides examples of common link load balancing solutions using the Link Controller.
- **BIG-IP e-Commerce Guide version 4.5 (optional)**
  This guide provides detailed configuration information for BIG-IP e-Commerce Controller systems.
- **Release notes**
  Release notes for BIG-IP version 4.6 are available from the product web server home page, and are also available on the technical support site. The release notes contain the latest information for BIG-IP version 4.6, including a list of new features and enhancements, a list of fixes, and, in some cases, a list of known issues.
- **Online help**
  You can find help online in three different locations:
  - The web server on the product has PDF versions of the guides included in the Administrator Kit.
  - The web-based Configuration utility has online help for each screen. Simply click the **Help** button.

- Individual **bigpipe** commands have online help, including command syntax and examples, in standard UNIX man page format. Simply type the command followed by the word **help**, and the BIG-IP system displays the syntax and usage associated with the command.

Stylistic conventions

To help you easily identify and understand important information, our documentation uses the stylistic conventions described below.

Identifying new terms

To help you identify sections where a term is defined, the term itself is shown in bold italic text. For example, a ***virtual server*** is a specific combination of a virtual address and virtual port, associated with a content site that is managed by a BIG-IP system or other type of host server.

Identifying references to objects, names, and commands

We apply bold text to a variety of items to help you easily pick them out of a block of text. These items include web addresses, IP addresses, utility names, and portions of commands, such as variables and keywords. For example, with the **bigpipe pool <pool_name> show** command, you can specify a specific pool to show by specifying a pool name for the **<pool_name>** variable.

Identifying references to other documents

We use italic text to denote a reference to another document. In references where we provide the name of a book as well as a specific chapter or section in the book, we show the book name in bold, italic text, and the chapter/section name in italic text to help quickly differentiate the two. For example, you can find information about load balancing methods in the ***BIG-IP Reference Guide***, Chapter 4*, Pools.*

Identifying command syntax

We show complete commands in bold Courier text. Note that we do not include the corresponding screen prompt, unless the command is shown in a figure that depicts an entire command line screen. For example, the following command shows the configuration of the specified pool name:

```
bigpipe pool <pool_name> show
```

or

```
b pool <pool_name> show
```

Table 1.1 explains additional special conventions used in command line syntax.

Item in text	Description
\	Indicates that the command continues on the following line, and that users should type the entire command without typing a line break.
< >	Identifies a user-defined parameter. For example, if the command has **<your name>**, type in your name, but do not include the brackets.
|	Separates parts of a command.
[ ]	Indicates that syntax inside the brackets is optional.
...	Indicates that you can type a series of items.

Table 1.1 *Command line syntax conventions*

2

SSL Proxy Selective Re-encryption

- Selective re-encryption at the pool level

Selective re-encryption at the pool level

One of the functions of the SSL proxy is to handle encryption and decryption tasks that are normally performed by a web server as part of processing a client request. When configured as a client-side-only proxy, the proxy decrypts incoming requests before sending them on in plain text to the target server. When the SSL-to-Server feature is enabled, the proxy provides an additional level of security by re-encrypting the request before sending it on to the target server.

SSL proxy server-side re-encryption at the pool level allows you to override the re-encryption option for selected pools. This is useful for configurations that include a local pool that does not require server side re-encryption and a remote fallback pool that requires server-side re-encryption. In order for selective re-encryption to function correctly, the pool must be referenced by a proxy that has server-side re-encryption enabled. For information on setting up server-side re-encryption on a proxy, see the ***BIG-IP Reference Guide***.

To configure selective re-encryption for a pool using the Configuration utility

Follow these steps to configure SSL server-side re-encryption on a pool using the Configuration utility. SSL server-side re-encryption is enabled by default.

1. In the navigation pane, click **Pools**.
   The Pools screen opens.
2. In the **Pool Name** list, click the pool name for which you want to set up SSL server-side re-encryption.
   This displays the properties of that pool.
3. Check the **Enable ServerSSL** box to enable SSL server-side re-encryption. Clear the **Enable ServerSS**L box to disable this feature.

To configure selective re-encryption for a pool from the command line

The **serverssl** option enables and disables the server-side re-encryption feature for the pool being defined. SSL re-encryption is enabled by default for all server-side connections. If this option is set to **disable**, server-side re-encryption is disabled on the target pool even when server-side re-encryption is enabled on the proxy.

To configure server-side re-encryption for a pool from the command line, type the **bigpipe pool** command, using the appropriate arguments, as follows:

```
bp pool <pool_name> serverssl <enable | disable>
```

To view the status of server-side re-encryption for a pool from the command line, type the following **bigpipe pool** command:

```
bp pool <pool_name> serverssl show
```

3

Node Counting Rule Function

The active_nodes function

This version of the BIG-IP software includes a new rule function, **active_nodes**(), that you can use to select a pool based on how many nodes are available in that pool.

For a node to be considered available, it can not be forced **down** or marked **down** by a monitor. The node must also have a valid route, and must not have exceeded the connection limit configured for the node. If there are no nodes available in a pool, the **active_nodes** function returns a zero (**0**).

The **active_nodes** function is useful for configuring rules that load balance traffic according to the number of nodes that are available for load balancing on a server or group of servers. For instance, if you have traffic going to a pool on a local server and a certain number of the nodes on a server go **down**, traffic can be automatically sent to a pool in another data center.

To configure a rule to select a pool based on how many nodes are available in a pool, use the syntax shown in the example in Figure 3.1. The expression is indicated in boldface.

```
rule my_rule {
     if (active_nodes (local_servers_pool) < 3) {
         use pool remote_proxy_pool
     }
     else {
         use pool local_servers_pool
     }
}
```

Figure 3.1 *Example of the active_node expression specified within a rule*

In Figure 3.1, the element **local_servers_pool** is the variable operand. The element < is the relational operator, and the element **active_nodes()** is the function. The expression evaluates to the integer **3**.

◆ **Note**

*If the **<pool_name>** specified does not exist, or when an invalid number of nodes is specified a rule, the **active_nodes** function returns a **0**.*

Configuring the active_nodes function in a rule

You can use the Configuration utility or the command line utility to create a rule that uses the **active_nodes** function. For information on how to create pools and other types of rules, see the ***BIG-IP Reference Guide.***

To configure the active_nodes function using the Configuration utility

1. In the navigation pane, click **Rules**.
   The Rules screen opens.
2. Click the **Add** button.
   The Add Rule screen opens.
3. In the **Name** box, type a 1- to 31-character name.
4. In the **Type** box, select **Text Input**. The Rule Builder does not support the **active_nodes** function.
   When you select **Text Input**, a screen displays in which you can type the complete text of your rule.
5. When you have finished entering the rule, click **Done**.

To configure the active_nodes function from the command line

Syntax

The **active_nodes()** function takes the following argument:

```
active_nodes (<pool_name>)
```

where:

<pool_name> is the name of the target pool.

Example

This function is designed primarily to be used for directly selecting between pools. The following example of the **active_nodes** function returns a pool name:

```
bp rule <rule_name> {if (active_nodes (<pool1>) == 0) {use pool
<pool2>} else {use pool <pool1>}}
```

4

CRL Authentication Enhancements

- Understanding CRL authentication
- Configuring CRL distribution points

Understanding CRL authentication

When presented with a client certificate, the BIG-IP system sometimes needs to assess the revocation state of that certificate before accepting the certificate and forwarding the connection to a target server. We recommend that you use Online Certificate Status Protocol (OCSP) to perform client certificate verification. ***OCSP*** is an industry-standard protocol that ensures that the BIG-IP system always obtains real-time revocation status during the certificate verification process. For more information on how to configure OCSP, see the ***BIG-IP New Features Guide for PTF-04***, Chapter 2, *Online Certificate Status Protocol for the BIG-IP System*.

If your configuration prevents you from using OSCP, the BIG-IP system supports the use of CRL distribution points as an alternative to OCSP for use with its SSL proxy feature. A ***Certificate Revocation List*** (CRL) is a list of revoked client certificates, which a server system can check during the process of verifying a client certificate. CRLs can be stored on one or more LDAP servers.

Enhancements to CRL authentication

This release includes several enhancements to CRL functionality, including the addition of CRL management using distribution points, and a configurable update interval that refreshes CRLs at a specified interval.

Before you configure any of the following CRL features, you should review the section on *Authentication* in the ***BIG-IP Reference guide version 4.5***, Chapter 7.

◆ **Note**

These features are only configurable using the command line utility.

Configuring CRL distribution points

CRL distribution points are a mechanism used to distribute certificate revocation information across a network. Distribution points are Uniform Resource Identifiers (URIs) or directory names specified in certificates that identify how CRL information is obtained by the server. Distribution points can be used in conjunction with CRLs to configure certificate authorization using any number of LDAP servers.

Activating distribution points

To enable the CRL distribution point feature, type the **bigpipe proxy** command, using the following arguments:

```
bp proxy <ip_addr>:<service> [clientssl] crldp <enable |
disable>
```

To assign the LDAP base directory name for certificates that specify the CRL distribution point in directory name format, type the **bigpipe proxy** command, using the following arguments.

where:

<base_dn> is either a URI or directory name, depending on what is defined in the client certificate:

```
bp proxy <ip_addr>:<service> [clientssl] crldp ldapserver [<base
dn> <ldap server ip> <ldap port>]
```

In order for distribution points to work correctly, URIs and directory names specified in the proxy must match the names in the CRL exactly.

◆ **Tip**

If you are specifying a directory name that contains an equals sign, you need to use the following standard UNIX format: ***\"base_dn\"***.

Setting the update interval for CRL distribution points

CRL files can become outdated, and might need to be updated as often as every day, or as seldom as every 30 days. If your CRL file is out-of-date, the BIG-IP system rejects all certificates, both valid and invalid. Certificates are rejected until the SSL proxy fetches a new CRL. For this reason, it is important to keep your CRL files up-to-date at all times.

You can specify an update interval for CRL distribution points. The update interval for distribution points ensures that CRL status is checked at regular intervals, regardless of the CRL timeout. This helps to prevent CRL information from becoming outdated before the BIG-IP system checks the status of a certificate. To specify the update interval for CRL distribution points, type the **bigpipe proxy** command using the following arguments. The update interval setting is disabled by default (**0**).

```
bp proxy <ip_addr>:<service> [clientssl] crldp update interval
<0 or (5-60)>
```

Setting the time-to-live for retrievals

To set the time-to-live (TTL) in minutes for successful retrievals, type the **bigpipe proxy** command, using the following arguments. The default is **60** minutes.

```
bp proxy <ip_addr>:<service> [clientssl] crldp ttl OK <10 to
1440>
```

To set the TTL in minutes for failed retrievals, type the **bigpipe proxy** command, using the following arguments. The default is **5** minutes.

```
bp proxy <ip_addr>:<service> [clientssl] crldp ttl FAILED <1 to
60>
```

To set the TTL for pending retrievals, type the **bigpipe proxy** command, using the following arguments. The default is **1** minute.

```
bp proxy <ip_addr>:<service> [clientssl] crldp ttl PENDING <1 to
5>
```

Configuring CRL skip processing for CRL distribution points

When it is only necessary to check the user certificate, and not CRL distribution points for the entire CRL chain, you can enable **skip crlchain**. This option is disabled by default.

To enable the skip check feature, type the **bigpipe proxy** command, using the following arguments:

```
bp proxy <ip_addr>:<service> [clientssl] crldp skip crlchain
<enable | disable>
```

Allow the use of previously retrieved CRLs when current retrievals fail

When current CRL distribution point retrievals fail or are pending, you can allow the use of previously retrieved CRLs. This option is disabled by default.

To enable this feature, type the **bigpipe proxy** command, using the following arguments:

```
bp proxy <ip_addr>:<service> [clientssl] crldp allow failure
<enable | disable>
```

Index