



F5 TMOS Operations Guide



Unified intelligence, flexibility,
and programmability

TMOS is the underlying architecture common to
all BIG-IP products.



A message from Julian Eames, Chief Operations Officer and Executive Vice President, F5 Business Operations

Welcome to the F5 Operations Guide series.

Our series of operations guides address real-world scenarios and challenges. The content was written by the engineers who design, build, and support our products, as well as other F5 professionals—some former customers worked in the field and have firsthand experience.

While no document can anticipate every question or situation, F5 endeavors to provide a better understanding of your BIG-IP system and offer tools needed to address common issues and conditions.

In this guide you'll find recommendations, practices, and troubleshooting tips to keep your F5 products running at peak efficiency and elements that may be incorporated into your own run books.

F5 is pleased to offer industry-leading products and services, including world-class support, and welcomes your suggestions and feedback. Let us know how we can better serve you.

—Julian Eames



Contents

Quick Start Guides	1
Maintenance at a glance	1
Maintenance checklist	6
BIG-IP upgrade checklist	7

Acknowledgments	8
------------------------	----------

About this guide	9
Before using this guide	9
Limits of this guide	9
Navigating this guide	10
Glossary	11
Customization	11
Issue escalation	11
Feedback and notifications	11
Document conventions	11
Change list	13

BIG-IP iHealth	14
At a glance—Recommendations	14
Background	14
Procedures	22
To view QKVIEW file details	22
To view, download, and/or save the active connections graph	22
To download all graphs to your computer	22
To download any file to your local computer	22
To see the TMSH network information	22
To run QKVIEW and download a snapshot file using the Configuration Utility	23
To run QKVIEW and download a snapshot file at the command line	24
To view the list of QKVIEW command line options	24



TO RUN QKVIEW AT LOW PRIORITY	24
TO VIEW A FULL, UNTRUNCATED QKVIEW	24
TO UPLOAD YOUR QKVIEW FILE AND VIEW IT IN BIG-IP iHEALTH	25
Additional resources	26
<hr/>	
Operating Environment	28
At a glance—Recommendations	28
Background	28
Procedures	29
TO CHECK APPLIANCE TEMPERATURE USING BIG-IP iHEALTH	30
TO CHECK APPLIANCE TEMPERATURE USING TMSH IN BIG-IP iHEALTH	30
TO CHECK APPLIANCE TEMPERATURE USING TMSH AT THE COMMAND LINE	30
Additional resources	33
<hr/>	
Hardware Diagnostics	36
At a glance—Recommendations	36
Background	36
Procedures	37
TO CHECK YOUR HARDWARE STATUS USING BIG-IP iHEALTH	38
TO VIEW BIG-IP iHEALTH HARDWARE INFORMATION ON YOUR VIPRION CHASSIS DISPLAY	38
TO RUN PLATFORM _ CHECK IN ITS FULL CAPACITY AT THE COMMAND LINE	39
TO RETURN THE SYSTEM TO NORMAL OPERATION AT THE COMMAND LINE	39
TO RUN PLATFORM _ CHECK ON A SPECIFIC VIPRION BLADE	40
TO DETERMINE THE EUD VERSION ON YOUR BIG-IP SYSTEM AT THE COMMAND LINE	41
TO DOWNLOAD EUD IM AND CORRESPONDING MD5 CHECKSUM FILES	43
TO DOWNLOAD EUD ISO AND CORRESPONDING MD5 CHECKSUM FILES	43
TO CHECK INTEGRITY OF THE DOWNLOAD AT THE COMMAND LINE	44
TO INSTALL EUD FROM AN IM INSTALLATION PACKAGE AT THE COMMAND LINE	45
TO LOAD THE EUD ONTO A USB DRIVE AT THE COMMAND LINE	45
TO BOOT EUD SOFTWARE FROM A USB FLASH DRIVE	49
TO BOOT THE EUD INSTALLED ON THE BIG-IP SYSTEM	49
Additional resources	50



VIPRION	52
At a glance–Recommendations	52
Background	52
Procedures	59
TO FIND THE RIGHT PLATFORM GUIDE FOR YOUR VIPRION SYSTEM	59
TO ADD MANAGEMENT IP ADDRESSES USING THE CONFIGURATION UTILITY	59
TO ADD MANAGEMENT IP ADDRESSES USING TMSH AT THE COMMAND LINE	59
TO CONFIGURE MULTICAST NETWORK FAILOVER USING THE CONFIGURATION UTILITY	59
TO DETERMINE THE PRIMARY BLADE ON A VIPRION SYSTEM USING TMSH AT THE COMMAND LINE	60
TO SHUTDOWN COMMAND ON ALL VIPRION BLADES	60
TO REBOOT ALL VIPRION BLADES	61
TO REBOOT A SPECIFIC SLOT	61
TO VIEW WHICH BLADES ARE AVAILABLE	61
Additional resources	69

Drive Maintenance	71
At a glance–Recommendations	71
Background	71
Procedures	77
TO RUN SMART CHECK ON SSDs USING TMSH AT THE COMMAND LINE	78
TO DETERMINE THE NAME OF YOUR SSD AT THE COMMAND LINE	78
TO VIEW THE SSD ALLOCATION AND MONITOR THE SSD LIFESPAN USING THE CONFIGURATION UTILITY	79

BIG-IP Virtual Edition	84
At a glance–Recommendations	84
Background	84
Procedures	87
TO CHANGE THE HTTPS PORT USING TMSH AT THE COMMAND LINE	87
TO CHANGE THE SSH PORT USING TMSH AT THE COMMAND LINE	87
Additional resources	88



Licenses and Entitlement	90
At a glance–Recommendations	90
Background	90
Procedures	92
To REACTIVATE YOUR BIG-IP SYSTEM LICENSE USING THE CONFIGURATION UTILITY	92
To VIEW LICENSE INFORMATION AT THE COMMAND LINE	92
To INSPECT THE EXPIRATION DATE AT THE COMMAND LINE	93
To CHECK QUERY THE STATUS OF THE IP INTELLIGENCE AT THE COMMAND LINE	93
To REQUEST A PRODUCT LICENSE PROFILE FROM F5	94
To INSPECT THE EXPIRATION DATE USING THE CONFIGURATION UTILITY	96
To ACTIVATE A LICENSE USING THE MANUAL ACTIVATION METHOD	98
To RE-ACTIVATE THE LICENSE WITH THE ADD-ON REGISTRATION USING THE MANUAL ACTIVATION METHOD	99
To PROVISION A LICENSED MODULE USING THE CONFIGURATION UTILITY	100
Additional resources	101

Backup and Data Recovery	103
At a glance–Recommendations	103
Background	103
Procedures	110
To USE TMSH HELP SYS CONFIG AT THE COMMAND LINE	110
To VIEW A LIST OF EXISTING ARCHIVES USING THE CONFIGURATION UTILITY	111
To CREATE A UCS ARCHIVE FILE USING THE CONFIGURATION UTILITY	113
To DOWNLOAD AND COPY AN ARCHIVE TO ANOTHER SYSTEM USING THE CONFIGURATION UTILITY	113
To CREATE A UCS ARCHIVE FILE USING TMSH AT THE COMMAND LINE	114
To VIEW THE PROPERTIES OF AN ARCHIVE USING THE CONFIGURATION UTILITY	115
To RESTORE A CONFIGURATION IN A UCS ARCHIVE USING THE CONFIGURATION UTILITY	116
To RESTORE CONFIGURATION DATA USING TMSH AT THE COMMAND LINE	116
To RESTORE CONFIGURATION DATA ON A REPLACEMENT RMA UNIT USING TMSH AT THE COMMAND LINE	117
To RESTORE UCS ARCHIVES ON BIG-IP SYSTEMS RUNNING NEWER SOFTWARE VERSIONS	119
To DOWNLOAD AN ARCHIVE USING THE CONFIGURATION UTILITY	119
To UPLOAD AN ARCHIVE USING THE CONFIGURATION UTILITY	120
To DELETE AN ARCHIVE USING THE CONFIGURATION UTILITY	120



TO VIEW A LIST OF THE EXISTING SCFs ON THE BIG-IP SYSTEM USING TMSH AT THE COMMAND LINE	121
TO CREATE AND SAVE AN SCF ON THE BIG-IP SYSTEM USING TMSH AT THE COMMAND LINE	121
TO VIEW THE PROPERTIES AND CONTENTS OF THE SCF AT THE COMMAND LINE	122
TO RESTORE DATA FROM AN SCF USING TMSH AT THE COMMAND LINE	122
TO COPY CONFIGURATION DATA TO A DIFFERENT PLATFORM USING SCF	122
TO DELETE AN SCF USING TMSH AT THE COMMAND LINE	122
TO RESTORE THE BIG-IP CONFIGURATION TO THE FACTORY DEFAULT SETTING USING TMSH AT THE COMMAND LINE	123
Additional resources	124
Software Updates	126
At a glance—Recommendations	126
Background	126
Procedures	127
TO SIGN UP FOR SECURITY MAIL LISTS	127
TO SIGN UP FOR THE TechNews MAILING LISTS	127
TO GENERATE AN RSS FEED	128
TO FIND THE LATEST SOFTWARE VERSION FOR YOUR F5 PRODUCT	128
TO VIEW OPSWAT VERSION INFORMATION USING THE CONFIGURATION UTILITY (BIG-IP VERSIONS 11.2.1 AND LATER)	129
TO VIEW OPSWAT VERSION INFORMATION USING THE CONFIGURATION UTILITY (BIG-IP VERSIONS 11.0 - 11.2.0)	129
TO VIEW OPSWAT VERSION INFORMATION USING TMSH AT THE COMMAND LINE	130
TO VIEW OPSWAT VERSION INFORMATION AT THE COMMAND LINE	130
TO VIEW OPSWAT VERSIONS AVAILABLE AT THE COMMAND LINE	131
TO VIEW AVAILABLE OPSWAT VERSIONS AT THE COMMAND LINE	131
TO INSTALL AN OPSWAT HOTFIX FROM THE CONFIGURATION UTILITY (BIG-IP APM 11.2.1 AND LATER)	131
TO INSTALL AN OPSWAT HOTFIX USING TMSH AT THE COMMAND LINE (BIG-IP APM 11.0 AND LATER)	132
TO DOWNLOAD AND INSTALL AN UPDATE TO THE IP GEOLOCATION DATABASE	134
TO INSTALL THE GEOLOCATION DATABASE UPDATE AT THE COMMAND LINE	134
TO COMPARE INODE NUMBERS AT THE COMMAND LINE	136
TO VERIFY THE SECURITY CONTEXT OF THE DATABASE FILES IN THE /SHARED/GeoIP DIRECTORY AT THE COMMAND LINE	137
TO RESTORE THE PROPER SELINUX SECURITY CONTEXT TO THE GEOLOCATION DATABASE FILES	137
TO CONFIGURE BIG-IP ASM TO DOWNLOAD ATTACK SIGNATURE UPDATES USING SCHEDULED UPDATE MODE	139
TO CONFIGURE BIG-IP ASM TO DOWNLOAD ATTACK SIGNATURE UPDATES USING MANUAL UPDATE MODE	139



To CONFIGURE BIG-IP ASM TO USE ATTACK SIGNATURES FROM MANUALLY DOWNLOADED UPDATES	140
To CONFIGURE SIGNATURE FILE UPDATES THROUGH AN HTTPS PROXY AT THE COMMAND LINE	141
Additional resources	142
<hr/>	
Networking and Cluster Health	144
At a glance—Recommendations	144
Background	144
Procedures	150
To VIEW CONFIGURATION DETAILS WITH THE CONFIGURATION UTILITY	150
To VIEW CONFIGURATION DETAILS AT THE COMMAND LINE	150
To VIEW THE STATISTICS ON THE PHYSICAL INTERFACES FROM THE CONFIGURATION UTILITY	150
To VIEW STATISTICS INFORMATION ON THE PHYSICAL INTERFACES AT THE COMMAND LINE	150
To VIEW VLAN CONFIGURATION INFORMATION THROUGH SIMPLE NETWORK MANAGEMENT PROTOCOL (SNMP)	150
To VIEW TMM ROUTES CONFIGURATION USING THE CONFIGURATION UTILITY	151
To VIEW TMM ROUTES CONFIGURATION AT THE COMMAND LINE	151
To VIEW THE ENTIRE TMM ROUTING TABLE AT THE COMMAND LINE	151
To VIEW TMM ROUTES CONFIGURATION THROUGH SIMPLE NETWORK MANAGEMENT PROTOCOL (SNMP)	151
To VIEW ARP CONFIGURATION THROUGH SIMPLE NETWORK MANAGEMENT PROTOCOL (SNMP)	151
To VIEW STATICALLY GENERATED ARP ENTRIES WITH THE CONFIGURATION UTILITY	151
To VIEW STATICALLY CONFIGURED ARP ENTRIES AT THE COMMAND LINE	152
To VIEW THE ENTIRE ARP TABLE AT THE COMMAND LINE	152
To VIEW IP CONFIGURATION WITH THE CONFIGURATION UTILITY	152
To VIEW IP CONFIGURATION AT THE COMMAND LINE	152
To VIEW CONFIGURED MANAGEMENT ROUTING AT THE COMMAND LINE	152
To VIEW THE MANAGEMENT ROUTING TABLE	152
To VIEW IP CONFIGURATION INFORMATION THROUGH SIMPLE NETWORK MANAGEMENT PROTOCOL (SNMP)	152
To VIEW NETWORK CONFIGURATION WITH THE CONFIGURATION UTILITY	153
To VIEW NETWORK CONFIGURATION AT THE COMMAND LINE	153
To VIEW SELF-IP CONFIGURATION INFORMATION THROUGH SIMPLE NETWORK MANAGEMENT PROTOCOL (SNMP)	153
To VIEW INTERFACE INFORMATION THROUGH SIMPLE NETWORK MANAGEMENT PROTOCOL (SNMP)	153
To VIEW VLAN CONFIGURATION DETAILS WITH THE CONFIGURATION UTILITY	153
To VIEW CONFIGURATION AT THE COMMAND LINE	154



To view statistics information for the interfaces assigned to the VLAN on the command line	154
To configure Network Failover with the Configuration Utility	154
To view trunk details with the Configuration Utility	154
To view trunk details at the command line	154
To view trunk statistics with the Configuration Utility	154
To view trunk statistics at the command line	154
To view trunks information through Simple Network Management Protocol (SNMP)	155
To configure the BIG-IP system to use an NTP server using TMSH at the command line	155
To use the NTPQ utility to query the NTP server and print a summary of the NTP server's state	155
To list the NTP servers configured on the BIG-IP system at the command line	158
To remove the NTP server configuration at the command line	158
Additional resources	158
<hr/>	
Log Files and Alerts	160
At a glance—Recommendations	160
Background	160
Procedures	166
To display the current SYSLOG facility levels	166
To configure the level of information, SYSLOG-NG sends to log files	166
To modify the LOGROTATE.LOGAGE database variable	167
To modify the number of archived log files	168
To configure a remote SYSLOG system at the command line	168
To create a custom SNMP trap at the command line	175
Additional resources	177
<hr/>	
Modules	179
At a glance—Recommendations	179
Background	179
Procedures	191
To disable BIG-IP AAM using the Configuration Utility	191
To delete DATASTOR application volume using the Configuration Utility	191
To provision SSDs for DATASTOR using the Configuration Utility	191



TO RE-ENABLE BIG-IP AAM USING THE CONFIGURATION UTILITY	191
TO MONITOR THE SSD LIFESPAN USING THE CONFIGURATION UTILITY	192
Additional resources	193
<hr/>	
MySQL	195
Background	195
Additional resources	195
<hr/>	
Caches	197
At a glance–Recommendations	197
Background	197
Procedures	199
TO DISPLAY THE CACHE SETTING ENTRIES FOR A PARTICULAR PROFILE AT THE COMMAND LINE	199
TO DISPLAY THE CACHE SETTING ENTRIES ON BIG-IP AAM AT THE COMMAND LINE	199
TO DETERMINE PERCENTAGE OF MEMORY USED BY EACH TMM PROCESS AT THE COMMAND LINE	199
TO VIEW DNS CACHE STATISTICS USING TMSH AT THE COMMAND LINE	199
TO DISPLAY STATISTICS FOR EACH TRANSPARENT CACHE USING TMSH AT THE COMMAND LINE	200
TO VIEW DNS CACHE STATISTICS USING THE CONFIGURATION UTILITY	200
TO VIEW DNS CACHE RECORDS USING TMSH AT THE COMMAND LINE	200
TO MODIFY CACHE STATISTICS USING THE CONFIGURATION UTILITY	200
TO INVALIDATE CACHE CONTENT USING THE CONFIGURATION UTILITY	202
TO ENABLE X-WA-INFO HEADERS USING THE CONFIGURATION UTILITY	202
Additional resources	206
<hr/>	
External APIs	208
At a glance–Recommendations	208
Background	208
Procedures	212
TO CONFIGURE A USER'S TMSH DEFAULT SHELL AT THE COMMAND LINE	213
TO CONFIGURE A USER'S TMSH DEFAULT SHELL USING THE CONFIGURATION UTILITY	213
TO CONFIGURE SELF IP PORT LOCKDOWN AT THE COMMAND LINE	214
TO CONFIGURE SELF IP PORT LOCKDOWN USING THE CONFIGURATION UTILITY	214
TO ASSIGN ICONTROL ADMINISTRATIVE RIGHTS TO A USER AT THE COMMAND LINE	214



TO ASSIGN iCONTROL ADMINISTRATIVE RIGHTS TO A USER USING THE CONFIGURATION UTILITY	214
TO CONFIGURE SELF IP PORT LOCKDOWN AT THE COMMAND LINE	215
TO CONFIGURE SELF IP PORT LOCKDOWN USING THE CONFIGURATION UTILITY	215
TO ASSIGN iAPPS ADMINISTRATIVE RIGHTS TO A USER AT THE COMMAND LINE	215
TO ASSIGN iAPPS ADMINISTRATIVE RIGHTS TO A USER USING THE CONFIGURATION UTILITY	215
TO CONFIGURE SELF IP PORT LOCKDOWN USING THE CONFIGURATION UTILITY	216
TO ASSIGN iCALL ADMINISTRATIVE RIGHTS TO A USER AT THE COMMAND LINE	216
TO ASSIGN iCALL ADMINISTRATIVE RIGHTS TO A USER USING THE CONFIGURATION UTILITY	217
TO CONFIGURE SELF IP PORT LOCKDOWN AT THE COMMAND LINE	218
TO CONFIGURE SELF IP PORT LOCKDOWN USING THE CONFIGURATION UTILITY	218
TO CONFIGURE SNMP AT THE COMMAND LINE	218
Additional resources	219
<hr/>	
Security	221
At a glance—Recommendations	221
Background	221
Procedures	228
TO SUBSCRIBE TO THE SECURITY UPDATES MAILING LIST	228
TO VIEW LOGIN ATTEMPTS USING THE CONFIGURATION UTILITY	228
TO VIEW LOGIN ATTEMPTS AT THE COMMAND LINE	228
Additional resources	229
<hr/>	
Optimize the support experience	231
F5 technical support commitment	231
F5 certification	232
Self-help	233
F5 global training services	236
Engage Support	237
TO LOCATE PLATFORM AND SYSTEM INFORMATION USING TMSH FROM THE COMMAND LINE	240
TO COPY SOFTWARE VERSION AND BUILD NUMBER INFORMATION FROM THE COMMAND LINE	240
TO COPY PROVISIONED MODULE INFORMATION FROM THE COMMAND LINE	241
TO REGISTER FOR WebSUPPORT PORTAL ACCESS	242



Legal Notices	244
Trademarks	244
Patents	244
Notice	244
Publication Date	244
Publication Number	244
Copyright	245

Appendix A: Outside the Box	246
Front panel characteristics	246
To find the appropriate guide for your BIG-IP or VIPRION platform	249
Back panel characteristics	250
VIPRION chassis characteristics	252

Appendix B: Deployment and Response Methodologies	254
At a glance—Recommendations	254
Background	255

Appendix C: Support Incident Report	265
Support Incident Report	265
Opening a Support Case	266



Quick Start Guides

The following pages are intended to help you hit the ground running if you need to quickly prepare for maintenance of your BIG-IP® system investment.

The quick start guides include:

- **Maintenance at a glance**, which compiles the recommendations and breaks them down by frequency and location of the procedures and background information in this document. We also provide a few external references.
- **Maintenance checklist**, which offers a set of tasks to help prepare for your BIG-IP maintenance periods.
- **BIG-IP upgrade checklist**, which provides a set of recommended tasks for preparing for BIG-IP upgrades.

There may be additional activities and tasks required by your company policies or industry standards that you may want to add to these lists.



Important These guides are intended to supplement your current business and systems operations and requirements. They are not intended to replace them.

Maintenance at a glance

One-time tasks

Description	See chapter	Notes
Ensure system is mounted properly according to platform guide.	Operating Environment	Platform guides are available by searching AskF5™ (support.f5.com).
Ensure the BIG-IP system synchronizes its clock with an NTP server.	Networking and Cluster Health	
Configure logging to remote log servers.	Log Files and Alerts	If you use centralized logging, ensure that the correct time and time zone are set on the device.
Configure SNMP traps.	Log Files and Alerts	
Set up a second power supply if your system has only one power supply.	Operating Environment	Not all platforms support multiple power supplies. Applies only to 1600, 2000, 3600, 4000, and 5000 series.
Connect redundant power supplies to two separate power sources in your data center.	Operating Environment	

**One-time tasks**

Description	See chapter	Notes
Subscribe to F5 TechNews and security mailing lists.	Software Updates or Optimize the support experience	See AskF5 Publication Preference Center (interact.f5.com/technews.html).
Become familiar with the initial baseline performance of your system.		<p>F5 recommends that you create a baseline for purposes of tracking performance changes over time. Also see platform data sheets for official baseline performance numbers determined by F5. (f5.com/resources/datasheets).</p> <p>Baseline data is offered for informational purposes and may not reflect the performance of your implementation.</p>

Daily tasks

Description	See chapter	Notes
Check available log files for messages pertaining to system stability and health.	Log Files and Alerts	
Review log files to identify and prevent excessive logging.	Log Files and Alerts	
Check debug modes to identify excessive logging and lower log rotation rate.	Log Files and Alerts	
Monitor the system (SNMP, iControl, script) for rapid increases in connections per second.	Networking and Cluster Health	Monitoring activity can identify possible Distributed Denial-of-Service (DDoS) attacks. F5 recommends sending data to an external monitoring system that can trigger alerts when values rise rapidly.

Weekly tasks

Description	See chapter	Notes
Upload a qkview file to iHealth.	BIG-IP iHealth	ihealth.f5.com
Check available disk space.	Drive Maintenance	

**Weekly tasks**

Description	See chapter	Notes
Check for software updates.	Software Updates	BIG-IP system versions 11.5 and later include an automatic update check feature. For more information, see AskF5 article: SOL15000: Using the Automatic Update Check feature . All BIG-IP system software can be obtained from F5 Downloads (downloads.f5.com).
View cache utilization.	Caches	

Twice-monthly tasks

Description	See chapter	Notes
Audit console messages to review logged messages.	Networking and Cluster Health	
Check neighbor routing table entries.	Networking and Cluster Health	Perform this task if your BIG-IP system is being used as a router.

Monthly tasks

Description	See chapter	Notes
Create a UCS archive and move to a storage repository.	Backup and Data Recovery	
Perform BIG-IP system change management review.	Backup and Data Recovery	
Check for OPSWAT updates.	Modules	
Check for attack signature updates.	Modules	
Review attack signature and policy settings.	Modules	

Quarterly tasks

Description	See chapter	Notes
Review iHealth trends.	BIG-IP iHealth	ihealth.f5.com Uploaded qkview data is deleted after three months. F5 recommends you back up and save this data to review trends over longer periods of time.

**Quarterly tasks**

Description	See chapter	Notes
Track data center and system temperatures as part of your review of BIG-IP iHealth qkview data.	Operating Environment	

Twice-yearly tasks

Description	See chapter	Notes
Perform facilities review: Verify ground lugs are attached to solid earth ground. Evaluate current and projected needs for rack space, power, HVAC, and so on. Consider virtualization and other potential optimizations.	Operating Environment	
Verify system entitlement, check for license expiration, and validate compliance levels.	Licenses and Entitlement	
Test BIG-IP ASM high-availability configuration and fail over under controlled environment.	Modules	Also do this before major application or configuration changes.
iRules code review.	Appendix B: Deployment and Response Methodologies	

Yearly tasks

Description	See chapter	Notes
Run diagnostics with platform check.	Hardware Diagnostics	In BIG-IP systems versions 11.4.0 and later, you can use the platform_check utility to collect SMART test data from the drive. The disk portion of the command output indicates Pass or Fail for the drive and logs detailed information to <code>/var/log/platform_check</code> .
Test failover systems as part of disaster recovery plan.	Backup and Data Recovery	

**Yearly tasks**

Description	See chapter	Notes
Check BIG-IP license service check date.	Modules	

As-needed tasks

Description	See chapter	Notes
Set data center humidity monitoring systems according to system platform guide.	Operating Environment	iHealth monitors do not measure humidity. Platform guides are available by searching AskF5 (support.f5.com).
Ensure proper airflow in data center and protect equipment from particulates.	Operating Environment	Be aware of airflow when moving equipment.
Perform capacity planning.	Operating Environment	
Create an SCF.	Backup and Data Recovery	Create and keep an SCF if you plan to copy a configuration across multiple BIG-IP systems.
Create UCS archive.	Backup and Data Recovery	Create an archive before and after making significant changes to your system before upgrading.
Check your system load when updating iRules.	External APIs	
Perform penetration testing.	Modules	Regular testing is recommended.
Review F5 customer training offerings and train staff.	Optimize the support experience	Review F5 customer training offerings and add to staff training schedule as needed. See F5 Certification (f5.com/education/certification) and F5 Training Programs and Education (f5.com/education/training).



Maintenance checklist

Using this checklist to plan your maintenance periods may ensure a better quality maintenance experience.

Timing	Recommended action	See
Before you begin maintenance.	Review and sign-off on your rollback process, including validation of rollover.	Backup and Data Recovery .
	Synchronize configurations.	Managing Configuration Synchronization in BIG-IP Device Clustering: Administration .
	Create a UCS archive for each BIG-IP system to be updated.	AskF5 article: SOL13132: Backing up and restoring BIG-IP configuration files (11.x) .
	Create a pre-maintenance baseline by generating a qkview file and upload to iHealth in case you need F5 support.	AskF5 article: SOL12878: Generating BIG-IP diagnostic data .
After maintenance.	Verify all pool members are up.	AskF5 article: SOL10516: Overview of BIG-IP pool status .
	Check high availability status table for anomalies.	AskF5 article: SOL9231: Overview of BIG-IP daemon heartbeat failover .
	Verify that your configuration loads.	At the command prompt, type: <pre>tmsh load sys configuration verify file</pre>
	Check log for errors.	Log Files and Alerts chapter in this guide.
	Verify that all monitors are online.	
	Ensure blades are online (VIPRION only).	VIPRION .
	Create a new qkview and upload to iHealth to compare with pre-maintenance baseline.	BIG-IP Health User Guide .



BIG-IP upgrade checklist

Before you upgrade your BIG-IP system software, review the release notes on [AskF5 \(support.f5.com\)](https://support.f5.com).

To find the release notes for your product

1. Go to [AskF5 \(support.f5.com\)](https://support.f5.com).
2. Under **Documentation**, click the product name.
3. From the **Product Documentation** menu, select your version.
4. Under **Release Notes**, click your version.

Completed	Research and preparation
<input type="checkbox"/>	Supported hardware.
<input type="checkbox"/>	Known issues.
<input type="checkbox"/>	Behavior changes.
<input type="checkbox"/>	Upgrade from earlier versions.
<input type="checkbox"/>	Installation checklist.
<input type="checkbox"/>	Review licensing information to ensure it's current.
<input type="checkbox"/>	Update as needed.
<input type="checkbox"/>	Confirm iRules and other automation is compatible with new version.



Acknowledgments

Executive sponsor: Julian Eames, Chief Operations Officer and Executive Vice President, F5 Business Operations

Publisher and project manager: Jeanne Lewis

Content and production editor: Andy Koopmans

Writers, editors, and testers: Justin Calhoun, Alex Chen, Anne DeJarnette, Eric Flores, Leroy Fumetti-Levine, Mike Kahler, Barb Hayes, Cathy Rodriguez, Keith Bowers, Ben Brandt, Jordan Zebor, Ilana Trager, Don Flinspach, Amy Wilhelm, Josh Michaels, Matt DuHarte, Bill Crawford, Dave Thomas, Michael Willhight, and Angus Glanville

BookSprints team: Juan Carlos Gutiérrez Barquero and Julien Taquet

Content, support, and assistance: Don Martin, Vice President, Global Services Strategic Programs; the Global Services New Product Introduction Team, Bryan Gomes, Phillip Esparza, Derek Smithwick, Beth Naczkowski, Joe Taylor, Mark Kramer, Andrew Pemble, Dave Bowman, Jim Williams, David Katz; and the rest of the Global Services management team; Angi Ghorbani, Bill Booth, Deepak Kumar, and the members of the F5 Test team; Ignacio Avellaneda, Colin Hayes, and Marian Salazar; Jill Durand, Ed Rabago, and the Portland F5 User's Group; Nathan Bultman and the AskF5 team; Kenneth Salchow and the F5 Certification team; Laura Michael, Brent Comer, and the F5 TechPubs team; Portland Users Group, our "Beta" readers from F5 Professional Certification Program and others.



About this guide

This guide includes recommended maintenance and monitoring procedures related to F5® TMOS 11.x–12.0.

The goal of this guide is to assist F5 customers with keeping their BIG-IP system healthy, optimized, and doing as designed. It was written by F5 engineers who assist customers with solving complex problems every day. Some of these engineers were customers before joining F5. Their unique perspective and hands-on experience has been used to serve the operational and maintenance guides F5 customers have requested.

This guide describes common information technology procedures and some that are exclusive to BIG-IP systems. There may be procedures particular to your industry or business that are not identified. While F5 recommends the procedures outlined in this guide, they are intended to supplement your existing operations requirements and industry standards. F5 suggests that you read and consider the information provided to find the procedures to suit your implementation, change-management process, and business-operations requirements. Doing so can result in fewer unscheduled interruptions and higher productivity.

See [Feedback and notifications](#) for information on how to help improve future versions of the guide.

Before using this guide

You will get the most out of this guide if you have already completed the following, as appropriate to your implementation:

- Installed your F5 platform according to its requirements and recommendations. Search the [AskF5 Knowledge Base \(support.f5.com\)](#) for “platform guide” to find the appropriate guide.
- Followed the general environmental guidelines in the hardware platform guide to make sure of proper placement, airflow, and cooling.
- Set recommended operating thresholds for your industry, accounting for seasonal changes in load. For assistance, you can contact [F5 Consulting Services](#).
- Familiarized yourself with F5 technology concepts and reviewed and applied appropriate recommendations from [F5 BIG-IP TMOS: Operations Guide](#).

Limits of this guide

This guide does not address installation, setup, or configuration of your BIG-IP system or modules.

There is a wealth of documentation covering these areas in [AskF5 Knowledge Base \(support.f5.com\)](#). The F5 self-help community, DevCentral ([devcentral.f5.com](#)), is also a good place to find answers about initial deployment and configuration.

The following figure shows where this guide can best be applied in the product life cycle.



Figure 0.1: F5 documentation coverage

Navigating this guide

Most chapters in this guide contain the following sections, each intended for a specific audience:

- *At a glance—Recommendations.* A list of recommended actions. Technicians may use this to find and complete maintenance tasks quickly. Engineers can review the list to determine which tasks are appropriate for the organization to adopt or customize, based on business requirements and policies.
- *Background.* Context for the subject matter and an understanding of issues related to recommended tasks. Engineers may use this in conjunction with Additional resources when designing, analyzing, and maintaining a network.
- *Procedures.* Instructions technicians may follow to carry out maintenance and monitoring tasks.
- *Additional resources.* List of F5 resources to help engineers and administrators dive deeper.



Glossary

A glossary is not included in this document. Instead, the [Glossary and Terms page](https://f5.com/glossary) (f5.com/glossary) offers an up-to-date and complete listing and explanation of common industry and F5-specific terms.

Customization

Customization may benefit your implementation. You can get help with customization from a subject matter expert, such as a professional services consultant from [F5 Consulting Services](https://f5.com/support/professional-services) (f5.com/support/professional-services).

Issue escalation

See [Optimize the support experience](#) for issue escalation information. Customers with websupport contracts can also open a support case by clicking **Open a support case** on the [AskF5 Knowledge Base](#) page (support.f5.com).

Feedback and notifications

F5 welcomes feedback and requests. You are invited to fill out and submit the surveys at the end of each chapter in the interactive PDF version of this guide. You can also send mail to opsguide@f5.com or visit the [F5 Operations Guide User Feedback survey](#). (This link sends you to an external site.)

F5 operations guides are updated frequently and new guides are being written. If you would like to be notified when new content is available, email opsguide@f5.com and your name will be added to our distribution list for updates and new releases.

Document conventions

To help you easily identify and understand important information, the document in this guide uses the stylistic conventions described here.

Examples

All examples in this document use only private IP addresses. When you set up the configurations described, you will need to use valid IP addresses suitable to your own network in place of our sample addresses.

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 interface labels, file names, specific web addresses, directories, and IP addresses.



Note Unless otherwise noted, all documents referenced in this guide can be found by searching by title at AskF5 (support.F5.com).

Configuration utility

The BIG-IP® Configuration utility is the name of the graphic user interface (GUI) of the BIG-IP system and its modules. It is a



browser-based application you can use to install, configure, and monitor your BIG-IP system.

Configuration utility menus, sub-menus, links, and buttons are formatted in bold text. For more information about the Configuration utility, see [Introducing BIG-IP Systems](#) in [BIG-IP Systems: Getting Started Guide](#).

Command line syntax

We show command line input and output in courier font. The corresponding prompt is not included. For example, the following command shows the configuration of the specified pool name:

```
tmsh show /ltm pool my _ pool
```

The following table explains additional special conventions used in command-line syntax:

Table 0.1 Command-line syntax

Character	Description
<>	Identifies a user-defined variable parameter. For example, if the command has <your name> , type in your name but do not include the brackets.
[]	Indicates that syntax inside the brackets is optional.
...	Indicates that you can type a series of items.

TMOS shell syntax

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

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

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

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

- You can open tmsh by typing tmsh at the BIG-IP system prompt:

```
(tmsh)#
```

Once at the tmos prompt, you can issue the same command syntax, leaving off tmsh at the beginning.



Note You can use the command line utilities directly on the BIG-IP system console, or you can run commands using a remote shell, such as the SSH client or a Telnet client. For more information about command line utilities, see [Bigpipe Utility Reference Guide](#) or the [Traffic Management Shell \(tmsh\) Reference Guide](#).

Change list

Date	Chapter/Section	Change	Reason
August 2015	All	Updates to formatting Addition of surveys	New Operations Guide style.
August 2015	Table 4.6	Fixed link	Misdirected link
November 2015	All	Revision for style Updates for BIG-IP 12.0	12.0 release



BIG-IP iHealth

At a glance—Recommendations

F5 has identified the following iHealth recommendations:

- Collect qkview files from each BIG-IP system.
- Upload qkview files to BIG-IP iHealth and review recommended maintenance and alerts to identify actionable items.
- Review qkview data trends on a regular basis.



Note If you choose not to use BIG-IP iHealth, you can provide your qkview diagnostic file to F5 Technical Support. For more information, see [Share diagnostic files with F5 technical support](#).

Background

This section provides context for our recommended procedures in the form of overviews and supplemental information.

BIG-IP iHealth overview

[BIG-IP iHealth \(iHealth.f5.com\)](#) is freely available to customers running BIG-IP version 10.x and later or Enterprise Manager™ version 2.x and later. It enables you to verify operation of your BIG-IP system and ensure your hardware and software function at peak efficiency by providing information covering your hardware, software, licensing, configuration, best practices, and known issues.

BIG-IP iHealth is a hosted application that parses a **qkview** file. The qkview file provides a running snapshot of your BIG-IP system with up-to-the-minute configuration and diagnostic information. You can download a qkview file from your BIG-IP system and then upload the file to the BIG-IP iHealth system.

BIG-IP iHealth provides outputs from commands running at the time a qkview snapshot is taken, the ability to graph system use and network traffic, software module details, and End of Life information for both hardware and software.

The BIG-IP iHealth system translates the output from your qkview file and displays the content in a customer-friendly format that mimics the familiar BIG-IP Configuration utility. In addition to translating the raw data, the BIG-IP iHealth Diagnostics component of the BIG-IP iHealth system evaluates the logs, command output, and configuration of your BIG-IP system against a database of known issues, common mistakes, and published F5 recommended practices. The prioritized results provide custom-tailored information specific to your configuration, along with recommendations for resolution, and a link to further information in the [AskF5 Knowledge Base](#).

qkview frequency

F5 recommends that you download a qkview file from your BIG-IP system and upload it to iHealth on a weekly basis. The F5 iHealth team updates diagnostics once a week and issues arising from the BIG-IP iHealth diagnostic output should be



addressed at the earliest opportunity.

Regularly uploading a qkview to BIG-IP iHealth can help you prevent unplanned outages by exposing risks. BIG-IP iHealth diagnostics help you resolve common configuration issues without F5 Technical Support's assistance. If you require additional support, F5 engineers can provide a rapid resolution using your BIG-IP iHealth data.



Note The BIG-IP iHealth web application interface may change; see the [BIG-IP iHealth User Guide](#) for details.

To use BIG-IP iHealth you must have access to the BIG-IP system's command line or the Configuration utility.

BIG-IP iHealth interface

When you log in to BIG-IP iHealth, the **Quick Information** bar loads, providing a list of all qkview files you have uploaded. **MyQkviews** displays by default. You can select other views, including **Saved Comparisons**, **Shared Qkviews**, **Hidden Qkviews**, and **Recently Viewed Qkviews**. Depending on the view, you can sort your files by **Hostname**, **Generation Date**, **Description**, or **Upload Date**. If you have uploaded a lot of files, you can also search by qkview name using **Find Qkview**.

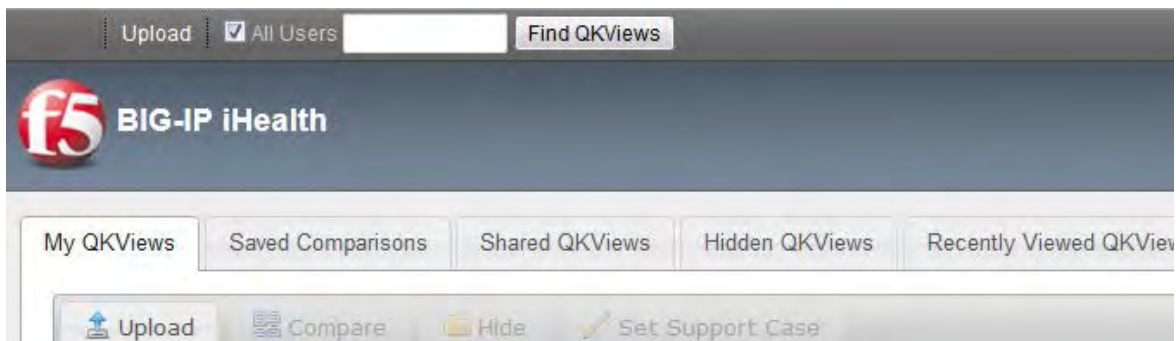


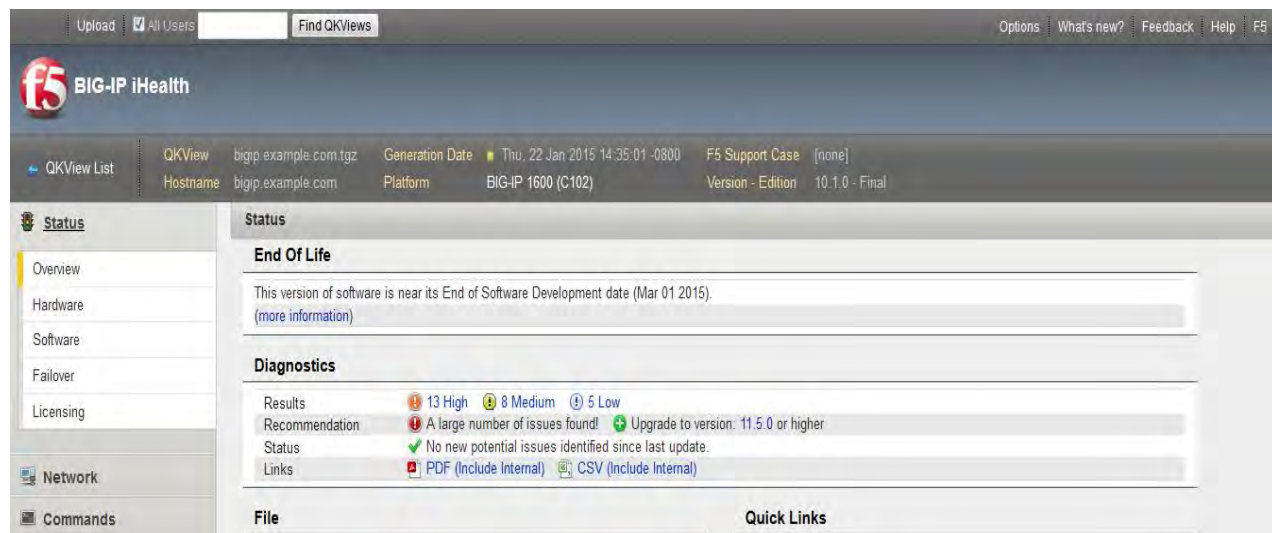
Figure 2.1 Quick Information bar

Quick Information bar

The following table describes items in the Quick Information bar.

Table 2.1 Quick information bar items

Item	Description
qkview	Name of the qkview file.
Hostname	Hostname of the associated qkview file. For VIPRION systems, the Hostname field allows you to select each individual blade and the chassis for diagnostic review.
Version	Software version including hotfix name.
Generation Date	Date and time the qkview file was created.
F5 Support Case	SR number associated with this qkview file.
Description	Description and identifier of the platform
Upload Date	Shows when qkview file was uploaded.
Comments	The first time the feature is used, a plus sign (+) appears next to Comments signifying that there are no comments. After comments have been entered, the icon becomes a page icon. This feature provides a space for annotating a qkview to help provide context upon future reviews.



The screenshot displays the BIG-IP iHealth interface. At the top, there's a navigation bar with 'Upload', 'All Users', and 'Find QKViews'. Below this, the 'BIG-IP iHealth' logo is visible. The main content area is divided into a left sidebar and a main panel. The sidebar includes links for 'QKView List', 'Status', 'Overview', 'Hardware', 'Software', 'Failover', 'Licensing', 'Network', and 'Commands'. The main panel shows the 'Status' overview, including 'End Of Life' information (software near its End of Software Development date) and 'Diagnostics' results. The diagnostics section shows 13 High, 8 Medium, and 5 Low issues, with a recommendation to upgrade to version 11.5.0 or higher. At the bottom, there are 'Quick Links' for PDF and CSV reports.

Figure 2.2 Status > Overview page



From this page, you can view a summary of BIG-IP iHealth diagnostic findings.

The menu on the left side of the page provides access to detailed information about the qkview file, including **Status**, **Network**, **Commands**, **Graphs**, **Diagnostics**, and **Files**.

Status menu

The **Status menu** contains information about the status of your system:

- **Overview**
- **Hardware**
- **Software**
- **Failover**
- **Licensing**

Status > Overview page

The **Status > Overview** page highlights key configuration data about your BIG-IP system:

Table 2.2: Areas of the BIG-IP iHealth Status > Overview page

Area	Description
End of Life	Tells you when the current version of the BIG-IP software will reach its End of Software Development date.
Diagnostics	Contains a summary of BIG-IP iHealth diagnostics findings.
Errors	Indicates whether there are any issues with the View file processing. It is only displayed in the event of an error
File	Lists details about the View file and any F5 Technical Support case numbers associated with the upload.
Quick Links	Provides quick access to configuration files and logs, such as the bigip.conf file.
System	Provides details about your BIG-IP system's hostname, time zone, chassis S/N, blade S/N, status, uptime, load average, physical memory, and CPU totals.
Licensing and Provisioning	This section provides a status of all software modules including product names, licensing status, provisioning status, and resource provisioning level.
ConfigurationTotals	Provides a total count of all virtual servers, nodes, pools, iRules, SNATs, NATs, and monitors associated with your configuration.
Software	Provides information about your product, including the current software version, with links to details regarding installed hotfixes



Status > Hardware page

The **Status > Hardware** page provides a snapshot of appliance information related to the system.

Specifications shows the specifications of your device.

Appliance shows **General information, Memory, CPU specs, Disks, Power Supplies, System information, Serial Numbers, Versions, Part Numbers, Additional Components**, and sensor data, if applicable.

VIPRION hardware is fully supported in BIG-IP iHealth. Each VIPRION blade has its own summary, with detailed disk partitioning information. The per-blade serial numbers aid in tracking chassis content. You can also identify mixed blade chassis on this page.

Status > Software page

The **Status > Software** page provides a snapshot of the installed software version, including licensing information for your F5 software, your Registration Key, and available firmware information.

Status > Failover page

The **Status > Failover** page outlines your network and hardware failover configuration data. This includes **Failover Type, Failover State, Unit ID, Active Time**, and high availability configuration information. Also included on this page are **Network, Unicast Configuration**, and **Hardware** failover port usage information.

Status > Licensing page

The **Status > Licensing** page provides a snapshot of all licensing information, including license and service check dates, **Registration Key**, and platform and appliance IDs. **Active Modules, Enabled Features**, and **Optional Modules** information is also included to help you understand your system.

Network menu

The **Network** menu allows you to dive into specific data about the configuration and status of your BIG-IP system at the time the qkview snapshot was taken. Each link opens a different view of the Network Map, which is a collapsible tree of your configuration objects.

You can open the **Network Map** directly to your virtual addresses, virtual servers, pools, pool members, iRules, profiles, classes, and monitors.

To see more information about any object, click its container folder. Object names that appear in strike-through type are offline. Hover over any object to view additional information about the state of your running configuration.

Commands menu

The **Commands** menu allows you to browse some commands as if they were typed at the command line. You can view Traffic Management Shell (tmsh), UNIX, and utilities command results.

Graphs menu

The **Graphs** menu allows you to view network activity in a variety of graphic displays, filtered by time period.



Note All data set names are described in the [F5 glossary](https://f5.com/glossary) (f5.com/glossary).

Diagnostics menu

The BIG-IP iHealth Diagnostics component automatically analyzes all custom diagnostics using your qkview data once the qkview file is uploaded to the BIG-IP iHealth system.

The **Diagnostics** menu contains four fields:

- Results lists issues summarized by level of importance (**Critical**, **High**, **Medium**, **Low**, or **Informational**).
- Recommendation lists software upgrade recommendations that may resolve potential issues discovered by BIG-IP iHealth.
- Status lists potential issues identified since the last software update.
- Links provides methods of viewing and downloading a diagnostics summary as a PDF or CSV file.



Note If BIG-IP iHealth does not find an issue of a particular importance level, that level will not be displayed in Results.

Results lists

You can view a complete list of results that BIG-IP iHealth discovered with your qkview file, filtered by importance level. From the Results summary, click the link associated with the importance level of results you want to see (for example, **High**). A list of results filtered by importance level is displayed.



The screenshot displays the BIG-IP iHealth Diagnostics page. The left sidebar contains a navigation menu with sections: Status, Network, Commands, Graphs, and Diagnostics. Under Diagnostics, there are filters for Importance (Critical (0), High (13), Medium (0), Low (0)), Status (Issues Found, Passed), Audience (External, Internal), and Tags (CVE). Below these are links for Downloads and Files. The main content area shows a list of diagnostic issues. Each issue entry includes a title, a Recommended upgrade version, Solution Links, Internal Solutions, and a Heuristic Name. The issues listed are:

- An SSH configuration error exposes a potential vulnerability - CVE-2012-1493**: Recommended upgrade version 10.2.4, 11.0.0.HF2, 11.1.0.HF3, 11.2.0.0. Solution Links: SOL13600. Internal Solutions: SOL13601. Heuristic Name: H380502.
- Various Java vulnerabilities**: Recommended upgrade version None. Solution Links: None. Internal Solutions: SOL14249. Heuristic Name: H389455. Marked as internal.
- IP randomization vulnerability CVE-2008-1146, CVE-2008-1147, CVE-2008-1148**: Recommended upgrade version None. Solution Links: None. Internal Solutions: SOL14139. Heuristic Name: H435621. Marked as internal.
- CRIME vulnerability via TLS 1.2 protocol CVE-2012-4929**: Recommended upgrade version 10.2.4.HF5, 11.1.0.HF5, 11.2.0.HF4, 11.2.1.HF4, 11.3.0.0. Solution Links: SOL14854. Internal Solutions: None. Heuristic Name: H435085.
- OpenSSL OCSP vulnerability CVE-2013-0166**: Recommended upgrade version 10.2.4.HF5, 11.1.0.HF5, 11.2.0.HF4, 11.2.1.HF4, 11.3.0.HF2. Solution Links: SOL14261. Internal Solutions: None. Heuristic Name: H413556.
- SSL client connections may fail**: Recommended upgrade version 10.2.4. Solution Links: SOL14758. Internal Solutions: None. Heuristic Name: H433513.
- TMM vulnerability CVE-2013-6016**: Recommended upgrade version 10.2.2.HF3, 11.0.0.HF1. Solution Links: SOL13233. Internal Solutions: None. Heuristic Name: H433824.
- MySQL Server vulnerability CVE-2012-3163**: Recommended upgrade version 11.4.0. Solution Links: SOL14907. Internal Solutions: None. Heuristic Name: H441052.

Figure 2.3 Diagnostics page



Tip In the list view, you may filter your results further by **Importance**, **Status**, **Audience**, and **Tags** from the left navigation menu. You may also download filtered reports in PDF or CSV formats from the **Downloads** dropdown menu.

Each issue in the list contains a title summarizing the issue, a Recommended upgrade version (if any), links to AskF5 solution articles that may help resolve or describe the issue, and a Heuristic Name.



Note **Heuristic Name** is a unique indicator providing F5 Technical Support with data about the BIG-IP heuristics engine processes for the diagnostics issue.



You can expand an individual issue to show more information by clicking **Details** in the issue pane or display the details for all listed issues by clicking **Show All**.

The detailed view includes a **Related Changes ID**, a more complete **Description** of the issue, a **Recommended** resolution (if applicable), and **Additional Information**.

The detailed view also contains a rating feature allowing you to rate whether the issue was helpful or not. F5 Technical Support uses rating information to update the diagnostics or to influence the development of other diagnostics.



Note If new diagnostics are added after you upload your qkview, the next time you access BIG-IP iHealth the new diagnostics will be run against your existing qkview and the results will be updated.

Files menu

Under the **Files** menu, you can drill down into all of the configuration files, logs, and other raw information contained in the qkview file. This information is unprocessed but may assist you in locating issues that were not found by the iHealth Diagnostics component.

Some information (such as large log files) may not be included in the qkview file.

Additional module-specific menus

Menu items for any additional modules that are licensed for your BIG-IP system also appear on the iHealth page. For example, a system licensed for the BIG-IP Application Security Manager™ (ASM) will display a **Security** menu, which gives an overview of each application security policy's settings.

Store qkview files

The BIG-IP iHealth system is intended as a diagnostic tool but. iHealth is not a solution for archiving operational data. Files uploaded to BIG-IP iHealth are maintained according to the F5 internal storage policy and will eventually be removed.

F5 recommends that you implement a storage solution for archiving your qkview files so that historical data can be used for comparison purposes and diagnostics.

Collect and archive qkviews

F5 recommends collecting and archiving qkview files from each BIG-IP instance on a weekly basis. You can but are not required to upload each qkview file to BIG-IP iHealth. Whether you upload them or not, we recommend archiving these files on a short-term basis. F5 Technical Support may compare a current qkview to a previous weekly qkview for insight into issues if they arise.



Procedures

This section details how to do the following BIG-IP iHealth tasks:

View qkview information

To view qkview file details

- Click the link for the file under Hostname.
- The **Status > Overview** page for the qkview file displays.

Work with graphs

To view, download, and/or save the active connections graph

1. Go to **Graphs > Active Connections**, then click **View Selected**.

The graph displays traffic for the 30 days prior to the creation of the qkview file.

2. To view other time periods, click the **7 day**, **1 day**, or **3 hr.** tabs above the graph.
3. To choose a custom time period, click **Custom** and type the time period you want to view.

You can also select individual data sets for the graph. This feature allows you to simplify and refine any graph to display a specific area of interest. When you have finished selecting the information of interest, click **Create Custom Graph**.

To download all graphs to your computer

1. Click **Download** at the top of the graphs.
2. To save an individual graph as PNG file on your computer, click the **Download** link at the bottom of the graph.

To download any file to your local computer

- Click the download icon next to the filename.
- If a filename is grayed out, the file contains no data.

View tmsh network information

To see the tmsh network information

1. Go to **Commands > tmshell> Network > list net interface all-properties –hidden**.

Results open in a new browser tab.



2. To view more than one command at a time, select the check boxes next to the commands you want to view, and then click **View As Group**.

Run qkview and download a snapshot file

You can run qkview and download a snapshot file with the BIG-IP Configuration utility or at the command line.

To run qkview and download a snapshot file using the Configuration utility

1. Log in to your BIG-IP system or Enterprise Manager Configuration utility.
2. Go to **System > Support**.
3. The qkview option is pre-selected.
4. Click **Start**.

The **Download Snapshot File** button will appear after a processing interval. This may take anywhere from a few moments to several minutes, depending on the current system load.

5. Click **Download Snapshot File** to download the output file.



Note The qkview utility runs a large number of commands when collecting information. This behavior may cause an additional performance burden on systems that are already heavily loaded.

**To run qkview and download a snapshot file at the command line**

- At the command prompt, type:

```
qkview
```

The output file name displays when the command has completed.

Collect the output file from the **/var/tmp/** directory, by copying the file to an external host using a utility such as FTP or secure copy (SCP).



Note The qkview utility runs a large number of commands when collecting information. This behavior may cause an additional performance burden on systems that are already heavily loaded.

In BIG-IP version 10.1.0 and later, you may run qkview by using the **tmsh run /util qkview** command.

qkview command line options**To view the list of qkview command line options**

- At the command prompt, type:

```
qkview -h
```

You can reduce the performance burden of qkview by running qkview at the lowest possible priority.

To run qkview at low priority

- At the command prompt, type:

```
nice -n 19 qkview
```

Large log files are often shortened to keep qkview file size down.

To view a full, untruncated qkview

- At the command prompt, type:

```
qkview -s0
```



Note On heavily loaded systems, qkview may take a long time to finish running when using **nice -n 19**.

Naming conventions for qkview files

The default name for a qkview file prior to BIG-IP version 11.4.0 is



```
case _ number###support _ file.tar.gz
```

In BIG-IP version 11.4.0 and later, the default file name is

```
case _ number _ ### _ support _ file.qkview
```

The latter file naming convention is used in all examples in this manual but instructions apply to files with either naming convention.

F5 recommends changing the default name to include your case number, if appropriate, and a count identifier.

For example:

```
c123456 _ A _ support _ file.qkview c123456 _ B _ support _ file.qkview
```

Upload your qkview file into BIG-IP iHealth

After you have obtained the qkview diagnostic file, you can upload the file to BIG-IP iHealth to diagnose the health and proper operation of your BIG-IP system.

To upload your qkview file and view it in BIG-IP iHealth

1. Go to [iHealth \(iHealth.f5.com\)](https://iHealth.f5.com).
2. Log in using your F5 WebSupport credentials.
3. Click **Upload**, then click **Choose**, and go to the location of the qkview file on your computer.

Optional If you have an open support case with F5 Technical Support, you can add it in the **F5 Support Case** field. If you do not have an open support case related to this qkview file, leave the field blank.

You can also add your own identifier to the **Description** field for tracking purposes.

4. Click **Upload** Qkview(s).

Once the upload has completed, the BIG-IP iHealth system may take several minutes to process the data.

Select your uploaded qkview files

You can log in to BIG-IP iHealth at any time to see a list of available uploaded qkview files. You can also access this list by clicking **MyQkviews**. Click the link for the qkview file you want to use and the BIG-IP iHealth overview page for that qkview file will display.



Note In MyQkviews, you can sort the columns by **Hostname**, **Generation**, **Date**, **Description**, or **Upload Date**. If you have uploaded several qkview files to the system, sorting the columns allows you to quickly find the qkview file you need.



Use Enterprise Manager to provide automatic uploads

BIG-IP iHealth is integrated with the Enterprise Manager system. You can configure the Enterprise Manager system to automatically create and upload qkview files (from your BIG-IP system or Enterprise Manager devices) to BIG-IP iHealth, and then view the diagnostics of all of your managed devices on a single screen.

Additional resources

The following table points to additional resources you can visit to learn more about the concepts and areas mentioned in this chapter. You can find AskF5 solution articles and the right product manuals for your software version by searching [AskF5 \(support.f5.com\)](https://support.f5.com).

Table 2.3: Additional resources

For more information about	See
Searching BIG-IP iHealth results.	BIG-IP iHealth User Guide
Comparing qkview files in BIG-IP iHealth.	BIG-IP iHealth User Guide
Monitoring network health in Enterprise Manager.	Enterprise Manager: Monitoring Network Health and Activity Manual

Help improve this guide

Please help F5 improve this guide by responding to a few questions about this chapter.

(Note: You must be viewing this document in Adobe Acrobat Reader or similar to use this form.)

Did this chapter answer all of your questions about the subject matter? Yes No

If not, what information should be included that is not? _____

Did you find any errors pertaining to subject matter in this chapter? Yes No

If yes, please describe the error: _____

If yes, please copy and paste the paragraph containing the error here: _____

Did you find non-subject-matter errors in this chapter (spelling, etc.)? Yes No

If yes, please describe the error: _____

If yes, please copy and paste the paragraph containing the error here: _____



Operating Environment

At a glance—Recommendations

F5 has identified the following operating environment recommendations:

- Track data center and system temperatures.
- Set data center humidity monitoring systems within specifications.
- Set up redundant power supply for systems with only one power supply and connect power supplies to separate power sources.
- Verify grounding lugs are still properly attached to a solid earth ground.
- Ensure proper airflow in data center and protect equipment from particulates.
- Ensure system is running within noise specifications.
- Ensure system is mounted properly.
- Perform capacity planning and environmental evaluation.

Background

This section provides context for our recommended procedures in the form of overviews and supplemental information. F5 appliances are designed to be run in a data center environment. They have broad specifications within that environment.

Platform guides

See specifications for your hardware in the appropriate platform guide for your BIG-IP system or VIPRION platform, available on [AskF5 \(support.F5.com\)](https://support.f5.com). To find the appropriate guide, enter the platform number from the front panel of your VIPRION device and “platform guide” in the search field.

Capacity planning

Having a healthy data center environment is important to the long-term health of your F5 hardware investment. Anticipating your ongoing power, space, network, and other resource needs can be determined by doing regular capacity planning. F5 suggests that you consider doing a capacity planning exercise at least once a year.



Recommended capacity planning may include the following procedures:

- Create a baseline inventory of your current server, storage and network infrastructure.
- Evaluate the needs required to support planned changes to your applications and network.
- Evaluate the “drift” or expected workload changes expected due to business growth or changes in your business cycle.
- Analyze the data collected and forecasting future infrastructure requirements and steps needed to meet them.

It is beyond the scope of this document to recommend a particular method of capacity planning.

Procedures

The following procedures instruct you how to do recommended monitoring for your BIG-IP system.

Environmental monitoring

F5 devices are tested at the maximum and minimum temperature and humidity combinations. The following table lists general platform environmental operating specifications for your reference.



Important Always check the appropriate platform guide for your device's particular specifications.

Table 3.1: General platform environmental operating specifications

Item	Specification
Operating temperature.	32 to 104°F (0 to 40°C).
Operational relative humidity.	10 to 90% (40°C).
Non-operational temperature.	-40 to 158°F (-40 to 70°C).
Non-operational relative humidity.	5 to 95% (40°C) non-condensing.



Temperature monitoring

Several temperature sensors are included in every F5 platform. They monitor the data center environment and the health of the appliance or chassis.

If the sensors on the air inlet temperatures indicate there is a problem, either the data center is too warm (check the platform guide for your device to see the exact limits), or the airflow to the rack or the specific device may be blocked.

A physical inspection and polling automated temperature-tracking systems within your data center is recommended.

To check appliance temperature using BIG-IP iHealth

1. In the **Status** menu, click **Hardware**.
2. On the **Appliance** tab, find the specs for **Temp** to verify that they are within the temperature guidelines specified in the appropriate platform guide for your device.

If data is not present, you can run the `tmsh` command, detailed in the next procedure.



Note BIG-IP iHealth heuristics report high-temperature conditions, but not all `qkview` files report temperatures other than that of the CPU.

To check appliance temperature using `tmsh` in BIG-IP iHealth

1. In the left navigation menu click **Commands**.
2. Click **tmsh**.
3. Click **System**.
4. Click show **/sys hardware**.

To check appliance temperature using `tmsh` at the command line

1. Log in to the Traffic Management Shell (tmsh) by typing the following command:

```
tmsh
```

2. At the command prompt, type:

```
show /sys hardware
```

Humidity monitoring

F5 devices can operate at a wide range of humidity, usually similar to or exceeding the other equipment in your data center. Very low humidity can cause excess static to build up, increasing the chance of damage to devices, and very high humidity can cause problems with condensation.



Grounding the hardware will provide additional safety for the hardware in the event of a short, as well as help reduce any static charge that builds up due to low humidity environments.



Important F5 devices themselves do not track humidity, so you will need to set your data center humidity monitoring systems to track humidity according to specifications given in the platform guide for your specific device(s).

Power source and electrical noise monitoring

Power is supplied to F5 systems through AC or DC power supplies. The power supplies used are determined at the time of your order, depending on how your data center is wired. The connections to your data center power distribution are important and must be monitored for safe and efficient use. The platform guide for your system includes installation instructions and specifications. Consult an electrician when necessary.

Earth grounding your F5 devices is very important for safety. All F5 appliances have a mechanism for grounding. As you make changes to your data center over time, verify that the grounding lugs are still properly attached to a solid earth ground.

F5 devices comply with various international electromagnetic compatibility standards for both emission and sensitivity to electrical noise. Check the platform guide for details for your region.

Redundancy

Many F5 devices have redundant power supplies, but some do not. The BIG-IP 1600, 3600, 3900, 2000, 4000, and 5000 series come standard with only one power supply. You may want to consider purchasing a second power supply for redundancy.



Important For devices with redundant supplies, connect the supplies to two separate power distribution points within your data center. This ensures that if one power distribution point has a problem, the appliance will remain up and running.

The exact specifications for the power source for each device will be found in the platform guide for your device. As you add equipment to and remove equipment from your data center, verify that you are still maintaining the proper current and voltage requirements for your device.



Airflow monitoring

Maintaining good airflow is critical to keeping your device working well. As equipment is moved around in a data center or other changes occur in the ventilation system, airflow intake and venting may change causing your F5 devices to overheat. Most F5 devices use front-to-back airflow, but some, notably the VIPRION 4000 series, use side-to-side airflow. Check your platform guide for a diagram of the airflow for your specific device.

Take care when labeling equipment or placing informational placards not to cover inlet or exhaust ports.

Data center equipment should be kept in an area with filtered air and low dust and particulates.

If your physical environment changes (construction work being done, for example), take care to protect your F5 appliances and your other data center equipment from dust. The airflow in most electronics will pull dust inside the chassis, and a buildup of dust can cause problems over time. The VIPRION C4800 has two air filters; check the corresponding platform guide for instructions on how to locate and periodically clean the filters. If dust has accumulated in the equipment, your regular BIG-IP iHealth checks likely will show a slow rise in internal temperatures, even if the inlet temperatures remain constant.

Acoustic noise monitoring

Acoustic noise may be an issue in some environments where there are specific standards for health and safety. F5 devices rarely function above normal limits for a data center. Check the specifications in the platform guide for your device to verify that it is within its normal limits.

Acoustic noise will increase over the lifetime of a device, so verify the operation of the fans with your periodic BIG-IP iHealth checks. Increased noise can indicate that a fan is not working properly, and most fans can be replaced as a field-replaceable unit (FRU).

Physical safety monitoring

As you make changes in your data center, you may move devices around to different racks or move them higher or lower within their existing racks. When doing so, check the platform guide for proper mounting options for your specific device(s) and verify that you have the correct hardware.

F5 chassis-based products come with lifting handles which should be used whenever devices are moved.



Important Take care not to lift chassis-based systems from areas like the fan assembly front panel or blade slots.

Some devices are quite heavy and require two or more people to move or re-install them. Check the platform guide for details on mounting hardware, placement instructions, and safety notes regarding weight and moving your device(s).



Additional resources

The following table points to additional resources you can visit to learn more about the concepts and areas mentioned in this chapter. You can find AskF5 solution articles and the right product manuals for your software version by searching [AskF5 \(support.f5.com\)](https://support.f5.com).

Table 3.2: Additional resources

For more information about	See
Environmental specifications for the 4000 series.	Platform Guide: 4000 Series
Environmental specifications for the 2000 series.	Platform Guide: 2000 Series
Environmental specifications for the 8900 system.	Platform Guide: 8900
Environmental specifications for the 6900 system.	Platform Guide: 6900
Environmental specifications for the 3600 system.	Platform Guide: 3600
Environmental specifications for the 8950 system.	Platform Guide: 8950
Environmental specifications for the 3900 system.	Platform Guide: 3900
Environmental specifications for the 1600 system.	Platform Guide: 1600
Environmental specifications for the 11050 system.	Platform Guide: 11050
Environmental specifications for the 11000 system.	Platform Guide: 11000
Environmental specifications for the 7000 series.	Platform Guide: 7000 Series
Environmental specifications for the 10000 series.	Platform Guide: 10000 Series
Environmental specifications for the 5000 series.	Platform Guide: 5000 Series
Environmental specifications for the 8400 and 8800 systems.	Platform Guide: 8400 and 8800
Environmental specifications for the 1500, 3400, 6400, and 6800 systems.	Platform Guide: 1500, 3400, 6400, and 6800
Environmental specifications for the VIPRION 2200 series.	Platform Guide: VIPRION 2200 Series



For more information about	See
Environmental specifications for the VIPRION 2400 system.	Platform Guide: VIPRION 2400 Series
Environmental specifications for the VIPRION 4400 series.	Platform Guide: VIPRION 4400 Series
Environmental specifications for the VIPRION 4800 system.	Platform Guide: VIPRION 4800 Series
Environmental specifications for the Enterprise Manager 4000.	Platform Guide: Enterprise Manager 4000
Environmental specifications for the VIPRION.	Platform Guide: VIPRION
Environmental specifications for the Enterprise Manager 500.	Platform Guide: Enterprise Manager 500
Environmental specifications for the Enterprise Manager 3000.	Platform Guide: Enterprise Manager 3000

Help improve this guide

Please help F5 improve this guide by responding to a few questions about this chapter.

(Note: You must be viewing this document in Adobe Acrobat Reader or similar to use this form.)

Did this chapter answer all of your questions about the subject matter? Yes No

If not, what information should be included that is not? _____

Did you find any errors pertaining to subject matter in this chapter? Yes No

If yes, please describe the error: _____

If yes, please copy and paste the paragraph containing the error here: _____

Did you find non-subject-matter errors in this chapter (spelling, etc.)? Yes No

If yes, please describe the error: _____

If yes, please copy and paste the paragraph containing the error here: _____



Hardware Diagnostics

At a glance—Recommendations

F5 has identified the following hardware diagnostic recommendations:

- Run diagnostics with BIG-IP iHealth and/or the platform_check utility.
- Use End-user diagnostics (EUD) software when recommended by F5.

Background

This section provides context for our recommended procedures in the form of overviews and supplemental information.

F5 has three tools you can use to check your hardware:

- BIG-IP iHealth (see [BIG-IP iHealth](#)).
- platform_check utility.
- EUD software.



Note Running EUD software requires a system reboot.

BIG-IP iHealth

BIG-IP iHealth can verify operation of most systems within the appliance or blade. It can check power, devices on the internal buses, disks, and memory.

platform_check utility

- Runs in a limited capacity every time a qkview is run.
- Provides hard drive SMART data as well as PCI bus address checking.
- Can check on additional system parameters.



Note To check additional parameters, all Traffic Management Microkernel (TMM) instances must be stopped.

To stop TMM instances, execute `bigstart stop` from the command line, which will interrupt all traffic processing. When the TMM instances are stopped, `platform_check` can check compression and SSL devices for relevant platforms. For more information about using `bigstart stop`, see AskF5 article: [SQL15442: Using the BIG-IP platform diagnostics tool](#).

EUD software

consists of a set of tests which report on various components in the hardware unit. The EUD is pre-installed on each BIG-IP system. Some parts of the hardware can only be checked if the system is offline and require the use of EUD. For compression hardware testing you must reboot into the EUD partition to run the EUD tests.

Procedures

Follow the procedures detailed in this section to guide you when doing hardware monitoring tasks.

Maintain hardware with BIG-IP iHealth

You can check hardware status through BIG-IP iHealth once you have run and upload a qkview file. From the **Hardware** menu in the left navigation menu. All hardware issues discovered by BIG-IP iHealth are listed under **Diagnostics**, ranked by severity or importance from **Low** to **Critical**.



Tip Verify your hardware on the same monitoring schedule as you collect your other BIG-IP iHealth data.



To check your hardware status using BIG-IP iHealth

1. Open the **Status > Hardware** page.
2. Check to see that the data for the following hardware monitoring fall within acceptable specifications for your platform:
 - Disks and power supply units.
 - Temperature, voltage, and fan speeds.
 - Physical RAM



Note RAM is measured as a power of ten (SI units) in platform guide documentation but displays in BIG-IP iHealth data in a power of two (IEC units). This can cause confusion in comparison. Make sure to convert measurements using an SI to IEC converter.

If you discover problems with your hardware, contact F5 Support. F5 Support may ask you to run EUD as part of diagnostics, so you should be prepared to take the system offline.

For VIPRION systems, BIG-IP iHealth data will be collected for all blades. Information on sensors is also available in the chassis display.

To view BIG-IP iHealth hardware information on your VIPRION chassis display

- Go to BIG-IP iHealth > **Procedures > Using BIG-IP iHealth > Status > Hardware for information.**

If you are using a qkview taken from a Virtual Clustered Multiprocessing® (vCMP®) guest, minimal hardware information is available and no information on sensors, disks, or other critical items is available. To view this data, you can upload a qkview file collected from the hypervisor, also called virtual machine manager (VMM).

For more information about using BIG-IP iHealth, see [BIG-IP iHealth](#).

Maintain hardware with platform_check

The platform_check utility can be used at the command line to verify that your hardware is operating properly. You should run the utility on a regular basis to make sure that you do not have any hidden problems on your hardware.



Important Standby systems should be checked regularly. Some issues may only become apparent when checked or when the primary fails over to the standby.



The `platform_check` utility can only check SSL and compression hardware on relevant platforms when Traffic Management Microkernel (TMM) instances are stopped. To stop TMM instances, run **bigstart stop** from the command line.



Note `platform_check` with TMM instances enabled is available in the **Commands** area of BIG-IP iHealth

To run `platform_check` in its full capacity at the command line

- At the command prompt, type syntax:

```
[root@spk:/S2-green-S:Active:Standalone] config # bigstart stop
[root@spk:/S2-(none)-S:INOPERATIVE:Standalone] config # run util platform_
check Disk Tests
SMART (/dev/sda): PASS SMART (/dev/sdb): PASS Hardware Acceleration Tests
Compression (0e:00.1):
PASS Compression (0e:00.2): PASS
....
SSL (0e:00.3): PASS SSL (0e:00.4): PASS
....
Miscellaneous Tests PCI: PASS Overall Platform Health: PASS
[root@spk:/S2-(none)-S:INOPERATIVE:Standalone] config # bigstart restart
[root@spk:/S2-green- S:Active:Standalone] config #
```

`platform_check` runs all diagnostics appropriate to your platform.

Once diagnostics are complete, you will need to return the system to its normal operating state.

To return the system to normal operation at the command line

- At the command prompt, type:

```
bigstart restart
```

Run `platform_check` on a specific component

If you want to run `platform_check` for only a specific component, use the **run util platform_check -h** command syntax

For example:

```
run util platform_check disk
```

This command runs only the disk suite of diagnostics.



Results data is provided on standard output as well as in the `/var/log/platform_check log` file. It is also available in xml format in the `/var/db/platform_check` file.

Run platform_check on a specific VIPRION blade

On a VIPRION, the SMART, compression, SSL, and PCI tests will run the same as on an appliance. The advantage of running platform_check rather than BIG-IP iHealth on a VIPRION is that traffic on other blades is unaffected while you can do deeper diagnostics.

To run platform_check on a specific VIPRION blade

- Log in to the console on the blade on which would like to do the test.



Important If you have vCMP guests running across the blade the throughput will be affected when you disable the TMM instances with `bigstart stop`. If any guests reside on this blade exclusively, they will stop working. If the blade you are testing is the primary, the primary will move to another blade in the system.



Maintain hardware with EUD

The EUD software is a set of tests that report on various components in the hardware unit. EUD is pre-installed on each BIG-IP system.

Use the correct and latest EUD software version

There are different EUD software packages available depending on your platform. For information about the latest EUD packages, see Ask F5 article: [SOL7172: Overview of EUD](#).

F5 recommends that you download and install the latest version of the EUD software for your platform prior to running system diagnostics. EUD software is updated regularly for the relevant platform types and contains fixes and up-to-date changes for supported hardware platforms. Older versions may not contain updates pertaining to platform changes such as those for RoHS compliance systems.



Important Failure to use the latest released version of the EUD may result in false negative or false positive reports. EUD reports containing false information or inaccuracies can delay the resolution of any potential underlying hardware problems.

Before running EUD software

- Do not run EUD software on a system that is in production. EUD software prevents traffic from passing during testing. Run EUD on a production system only if you are instructed to by F5 Support.
- Disconnect all network cables from the system. Any cables connected to the system during the tests could cause false-positive results.
- The B4300 blade allows additional EUD chassis back-plane data testing. EUD must run on two blades for this test. Running EUD on only one blade will result in test failure.

Download and install new EUD software

Before you download and install new EUD software, you should check to see which version you have installed on your BIG-IP system.

To determine the EUD version on your BIG-IP system at the command line

- At the command prompt, type:

```
eud _info
```

If you have EUD software installed, the version number appears.



Note You can also use this procedure to verify correct installation new EUD software

You have two options for downloading and installing EUD software:

- Download an ISO image burned burning it to a disk and boot from an external drive.
- Download and secure copy (SCP) an IM file to your BIG-IP system or a USB flash drive.

You will also need to download the MD5 **checksum** file to verify the ISO or IM file you downloaded.

Decide which files to download

There are several EUD file types available from the [F5 Downloads](https://downloads.f5.com) page (downloads.f5.com).

Table 4.1: File Types available for EUD download

File type	Description
ISO image	The ISO image is provided for burning a CD or DVD of the EUD. You can boot the CD/DVD from a powered USB CD/DVD drive plugged into the BIG-IP system.
IM files	The IM file is a self-extracting installation file. You can SCP this file directly to the BIG-IP system and use it to upgrade the EUD on the system or load a USB flash drive.
MD5 file	There is a corresponding MD5 file for each ISO image and IM file you download. Use the MD5 file to verify the integrity of the file you download.
Readme-EUD.txt	This file includes details about the release such as supported platforms.

**To download EUD IM and corresponding MD5 checksum files**

1. Go to the [F5 Downloads](https://downloads.f5.com) page (downloads.f5.com) and log in with your support ID.
2. Click **Find a Download**.
3. Under **F5 Product Family**, find **Hardware-Specific**, then click **Platform / EUD**.
4. Select your platform from the platform menu.
5. Click the name of the release with the most recent date.
6. Read and accept the software terms and conditions.
7. On the **Select a Download** page, click the file name **<file_name>.im**.
The **<file_name>** consists of the platform family and the build number.
8. On the **Download Locations** page, click a download location closest to yours and save the file to your computer.
9. Return to **Select a Download** page and download the corresponding MD5 checksum file. It will have the same name as the IM file with **.md5** as the file extension.

To download EUD ISO and corresponding MD5 checksum files

1. Go to the [F5 Downloads](https://downloads.f5.com) page (downloads.f5.com) and log in with your support ID.
2. Click **Find a Download**.
3. Under **F5 Product Family**, find **Hardware-Specific**, then click **Platform / EUD**.
4. Select your platform from the platform menu.
5. Click the name of the release with the most recent **Date**.
6. Read and accept the software terms and conditions.
7. On the **Select a Download** page, click the file name **<file_name>.iso**.
The **<file_name>** consists of the platform family and the build number.
8. On the **Download Locations** page, click a download location closest to yours and save the file to your computer.
9. Return to **Select a Download** page and download the corresponding MD5 **checksum** file. It will have the same name as the ISO file with **.md5** as the file extension.



Use downloaded EUD files

There are a few possible tasks you can do with downloaded EUD files.

Table 4.2: Possible tasks with downloaded EUD files

Task	Description
Use the MD5 checksum to verify the files.	Use the MD5 file to verify the integrity of the file you download.
Install the EUD from the IM installation package.	You can SCP this file directly to the BIG-IP® system and use it to upgrade the EUD on the system.
Load the EUD onto a USB flash drive.	Load the EUD onto a USB flash drive and run the EUD from the flash drive.

Check the integrity of the download with MD5 checksum

You can do this task after you download update files and their corresponding **.md5** files from the [F5 Downloads](https://downloads.f5.com) page (downloads.f5.com). Verify the MD5 **checksum** on each file you download using the **md5sum** command. Use the output to verify the integrity of the downloaded file.

To check integrity of the download at the command line

- At the command prompt, type:

```
md5sum -c <file _ name>.md5
```

Replace **<file name>** with the name of the file you downloaded.

If the output returns “OK,” the download was successful. If you receive any other output, you should download the file again and repeat the process.



Install the EUD from an IM installation package

You should copy the IM file to **/var/tmp** directory on the system you intend to update before you begin this procedure. Installing the EUD from an IM file is one method you can use to get the latest EUD installed on your hardware.

To install EUD from an IM installation package at the command line

- At the command prompt, type:

```
im <file _ name>.im
```

The latest EUD is installed on your hardware.

To load the EUD onto a USB drive at the command line

- Download the IM file to **/tmp/eud**.
- Loopback mount the IM file by typing the following command:

```
mkdir /tmp/eud; mount -o ro,loop <file _ name>.im/tmp/eud
```

Replace **<file name>** with the name of the file you downloaded.

- Insert a USB mass storage device into the platform on which you mounted the IM file.
- Run the **mkdisk** utility by typing the following command:

```
cd /tmp/eud; ./mkdisk
```

- Follow the prompts to load the EUD onto the USB flash drive. After the installation is complete, remove the USB flash drive from the BIG-IP system.

Run the EUD tests

There are two options for running the EUD tests. You must have a console connected to your BIG-IP system to run the EUD software.

Table 4.3: Options for running EUD tests

Task	Description
Boot the EUD from a USB flash drive.	Plug your EUD USB flash drive into the BIG-IP® system and boot to the EUD.



Task	Description
Run the EUD from the system boot menu.	As the system is booting, select the EUD option from the boot menu.

EUD test suite

The following table describes the various tests EUD software can do.

Table 4.4: EUD test suite

Test name	Description	Success message
PCI.	Reports on and verifies the PCI devices on the PCI bus. Tests the following devices: Host PCI, Host bridge. System peripheral, Communication controller, ISA bridge. RAID bus controller, SMBus controller. Signal processing controller, Network and computing encryption MIPS. USB controller, PCI bridge, Ethernet controller, Switch controller.	Test Complete: PCI Test PASSED.
ECC Status.	Checks ECC memory for error correction codes and reports single-bit or multi-bit errors.	Test Complete: ECC Status PASSED.
Internal Packet Path	Uses internal packet path to test Ethernet interfaces in system. Sends known payload packets from mainboard Ethernet interface back to mezzanine Ethernet interface. Checks for correct receive order and payload and then checks statistics at switchboard and HSB. Test takes approximately two minutes.	Test Complete: Internal Packet Path PASSED.
Internal Loopback	Sets front interfaces into PHY or MAC loopback mode and runs packets through path from switch chips.	Test Complete: Internal Loopback PASSED.
SSL	Tests SSL hardware.	



Test name	Description	Success message
Self-Monitoring Analysis and Report Technology (SMART)	<p>Tests internal status of hard drive, including:</p> <p>Read error rate start/stop count.</p> <p>Re-allocated sector count, Power on hours count, Spin-up retry count.</p> <p>Drive calibration retry count, Drive power cycle count.</p> <p>Offline scan uncorrectable sector count, Ultra ATA CRC error rate and multi-zone error rate</p>	Test Complete: SMART Test PASSED.
Power System	<p>Reports information about installed power supplies.</p> <p>Returns chassis voltage measurements, fan speeds, and mode of fan controller.</p>	Test Complete: Power System Test PASSED.
Hardware Firmware Update	<p>Updates hard drive firmware on BIG-IP 3900 and EM 4000 platforms. Appears only on these platforms when system is booted with older version of firmware.</p> <p>Important F5 recommends backing up configuration before running update.</p>	Test Complete: Mezzanine Packet Test PASSED.
System RAM	<p>Performs SDRAM data bus and address bus test. All available user memory tested.</p> <p>Runs following tests:</p> <p>Stuck address test.</p> <p>Random value test.</p> <p>XOR comparison test.</p> <p>SUB comparison test.</p> <p>MUL comparison test.</p> <p>DIV comparison test, OR comparison test, AND comparison test.</p> <p>Sequential increment test.</p> <p>Warning This test may take several hours to complete, depending on the amount of available memory.</p>	Test Complete: PASSED.
LED (Interactive)	<p>Sets each possible LED status levels and prompts to verify corresponding color and operation.</p> <p>Can be done from console or LCD panel.</p> <p>Important Some LED questions time out after a minute. If a question times out, the LED test fails.</p>	Test Complete: PASSED.



Test name	Description	Success message
LCD	Tests functionality of LCD panel. Requires access to LCD panel on the tested unit. You will need to respond to interactive prompts.	Test Complete: PASSED.
Mezzanine USB	Tests USB ports on mezzanine card installed in platform.	Test Complete: PASSED.
Mezzanine Packet	Treats HSB as standard Ethernet NIC card. Once NIC module/driver is loaded, does loop test by sending and receiving network packets over HSB network interface. Tests number of packets sent from one HiGig interface to another HiGig interface.	Test Complete: PASSED.



EUD options

You can specify the options listed in the following table to modify the EUD process.

Table 4.5 EUD options

EUD option	Description
A Run All (Non-Interactive) Tests	Runs all tests applicable to system except interactive tests.
I Run All Interactive Tests.	Runs LED and optional LCD tests.
D Display Test Report Log	Displays test report. A report log is stored as text file named /shared/log/eud.log in host file system. Important You must run eud_log at the command line to create output.
S Display Test Summary	Displays test summary report showing the results of all tests run during test session.
Q Quit EUD and Reboot the System	Stops the EUD and reboots the system. Warning Using other methods to stop the diagnostics, such as the reboot command or the command menu option can destabilize the system.

Boot the EUD from a USB flash drive

You must load the EUD image onto the USB flash drive to run the EUD from the drive.

To boot EUD software from a USB flash drive

1. Turn off the BIG-IP system.
2. Load the EUD image onto a USB flash drive.
3. Insert flash drive into USB port on BIG-IP system.
4. Turn on the BIG-IP system.

When the EUD starts, the EUD menu appears on the console.

Start the EUD from the boot menu

Install the latest version of the EUD before you boot the EUD from the boot menu.

To boot the EUD installed on the BIG-IP system

1. If the system is powered on, turn it off.
2. Power on the system. As the unit boots, it pauses briefly on the boot menu.



3. Use the arrow keys to highlight **End-user diagnostics**.
4. The EUD starts and the EUD menu appears on the console.

Additional resources

The following table points to additional resources you can visit to learn more about the concepts and areas mentioned in this chapter. You can find AskF5 solution articles and the right product manuals for your software version by searching [AskF5 \(support.f5.com\)](https://support.f5.com).

Table 4.6: Additional resources

For more information about	See
EUD testing empty SFP/SFP+ port on an 8900.	SOL14748: The EUD utility may incorrectly report a failure when testing an empty SFP/SFP+ port.
On a 2000,4000, 5000, or 7000 system, the EUD Verify Host I2C test fails.	SOL14640: The EUD 'Verify Host I2C' test may fail indicating a false positive hardware failure.
Determining the EUD version you are running.	SOL8002: Determining the end-user diagnostics version.
Running the EUD memory test without disconnecting all the network cables.	SOL13608: Running the EUD memory test may cause a bridge loop.
Considerations for running EUD on a VIPRION® platform.	SOL12942: The EUD Internal Packet Path Test may generate false positive results on VIPRION platforms.
Overview of the EUD software.	SOL7172: Overview of the end-user diagnostics software.
The EUD may pass when a hard disk is missing or undetected on a 6900 or 8900 platform.	SOL14078: The EUD may report a PASSED test when a hard drive is missing or undetected.
Creating a bootable USB drive from a Windows computer from an F5 appliance.	Devcentral: Create EUD on USB from Windows. Creating a Bootable USB Thumb Drive in BIG-IP Systems Getting Started Guide.

Help improve this guide

Please help F5 improve this guide by responding to a few questions about this chapter.

(Note: You must be viewing this document in Adobe Acrobat Reader or similar to use this form.)

Did this chapter answer all of your questions about the subject matter? Yes No

If not, what information should be included that is not? _____

Did you find any errors pertaining to subject matter in this chapter? Yes No

If yes, please describe the error: _____

If yes, please copy and paste the paragraph containing the error here: _____

Did you find non-subject-matter errors in this chapter (spelling, etc.)? Yes No

If yes, please describe the error: _____

If yes, please copy and paste the paragraph containing the error here: _____



VIPRION

At a glance—Recommendations

F5 has identified the following VIPRION recommendations:

- Ensure VIPRION is configured according to recommended practices.
- Determine the primary blade.
- Work from blade to blade (address the management port on any blade).
- See platform guide for maintenance activities.
- Monitor tasks that are different from a BIG-IP ADC.
- Add a blade and monitor its installation.
- Conduct failover management.
- Conduct blade migration.
- Create cluster traps.

Background

This section provides context for our recommended procedures in the form of overviews and supplemental information.

VIPRION platform maintenance

All VIPRION platforms contain several components that you can replace without exchanging the entire system. The list of components varies from one VIPRION platform to another. They may include:

- AC power supply
- DC power supply
- Fan tray
- Hard drive assembly
- Blades
- Bezel (with LCD component)
- Cable managers
- Chassis filter



- Power supply filter
- Annunciator cards

Detailed procedures for replacing these components are described in the platform guide for each VIPRION Series.

VIPRION standard operating states

Chassis standard operating states

When the VIPRION platform is in a standard operating state, the LEDs behave in a defined manner.

Table 5.1: LED indicators for chassis standard operating states

System state	Primary LED	Secondary LED	Status LED	Alarm LED
Active mode	Off/None	Off/None	Green solid	Off/None
Powered off	Off/None	Off/None	Off/None	Off/None

VIPRION platform guides

Platform Guides for each of the VIPRION models are available at [AskF5 \(support.f5.com\)](https://support.f5.com).

Each guide provides detailed information on the VIPRION platform, including:

- Chassis components
- Blade components
- LCD menus
- Chassis and blade standard operating states
- Blade LED status conditions
- Indicator LEDs
- LED alert conditions
- Platform interfaces
- Platform installation
- Platform maintenance
- Environmental guidelines
- Platform specifications



Note The LCD panel on both VIPRION 2000 Series platforms is available as a separate USB module.

Blade standard operating states

When the VIPRION platform is running in a standard operating state, the Status LED of each blade turns yellow on startup and turns green when the BIG-IP software has booted successfully.

Table 5.2: LED indicators for blade standard operating states

System state	Status LED	Alarm LED
Primary	Green solid	Off/None
Secondary	Green solid	Off/None
Powered off	Off/None	Off/None



Recommended practices for configuring your VIPRION

F5 recommends the following configuration practices for setting up your VIPRION.

Important considerations

- In All management ports must be cabled to allow access in the event the primary blade shifts. In BIG-IP v. 12.0
- Any blade in the chassis can be primary.
- The system has a cluster IP address that should be used as the management IP that is routed to the appropriate primary blade.
- When the primary blade shifts, the cluster IP address will always have access to the primary blade.
- You must have management access to each blade for blade-specific administrative activities and to configure a full high-availability mesh within a high-availability (HA) pair of VIPRION chassis.
- Assign a management IP address to every slot.

Use multi-blade aggregated links (trunks) for all VLANs

Always use aggregated links (trunks) for all VLANs. Aggregated links provide fault tolerance if one link goes down, and they can increase bandwidth as well.

If you configure the aggregated links to use interfaces on multiple blades, you remove a single point of failure if a blade becomes unavailable. The connections can remain up, even if one blade is missing.

Configure NTP

In multi-blade VIPRION high-availability (HA) pairs, NTP must be enabled. Time synchronization is critical both for inter-chassis communication and inter-blade communication.

The VIPRION uses Rsync for inter-blade communication, and system time must be maintained to ensure this communication is successful.

Ensure the serial ports on all blades are connected to a serial concentrator

Console connection is important for a VIPRION chassis for the following reasons:

- If a critical event causes a blade to go offline, console output supersedes any syslog type logging.
- EUD software needs console access to boot and do diagnostic tests.

In the event that the VIPRION chassis is not accessible through the network, console access will be required to determine root cause analysis and to restore services on the VIPRION.



Use an HA VLAN between chassis for heartbeat, connection mirroring, and persistence mirroring traffic

Having a dedicated network is important for the following reasons:

- Network failover is the only method to insure high availability. We recommend a network failover trunk with member interfaces from each blade of a VIPRION.
- Connection mirroring VIPRION traffic may use excessive resources due to the amount of traffic that can be handled from the hardware.

F5 recommends using a dedicated mirroring network to ensure successful connection mirroring.

- Ensure that each VIPRION in a sync-failover device service cluster has the same number and model of blades installed in each chassis. Configurations must be able to config-sync across the two chassis. Different blades use different addresses, trunks, and VIPs.
- Blades should be installed in the same position(s) in both chassis. For example, if one chassis in the sync-failover device group has blades in slots 1 and 2, then the other chassis should also have its blades installed in slots 1 and 2.
- Wire the management ports on all blades to the management network.

Use multicast network failover on the management network

If available, consider adding multicast network failover to the management network as a backup method to maintain high availability. For more information, see AskF5 article: [SOL13915: Configuring network failover for redundant VIPRION systems \(11.x\)](#).



VIPRION inter-blade administrative traffic

The VIPRION system is comprised of a cluster of blades that work together to process network traffic.

Each blade in a VIPRION system communicates by sending inter-blade administrative traffic over the management backplane. The blades are connected to the management backplane by the `mgmt_bp` interface, meaning the management backplane is distinct from both the data backplane and the management interface.

You can display interface statistics for the `mgmt_bp` interface by running the `ifconfig -a` command. For example, the following `mgmt_bp` interface statistical information was taken from slot 2 of a VIPRION system:

mgmt_bp	Link encap:Ethernet HWaddr 00:01:D7:71:CD:41	inet addr:192.0.2.2
Bcast:192.0.2.22 Mask:255.255.255.0		
inet6 addr: fe80::201:d7ff:fe71:cd41/64		
Scope:Link UP BROADCAST RUNNING MULTICAST		
MTU:4096 Metric:1		
RX packets:39088409 errors:0 dropped:0 overruns:0 frame:0 TX packets:37470798 errors:0 dropped:0 overruns:0		
carrier:0 collisions:0 txqueuelen:1000		
RX bytes:4141196638 (3949.3 Mb) TX bytes:694315251 (662.1 Mb)		
Interrupt:16		
mgmt_bp	Link encap:Ethernet HWaddr 00:01:D7:71:CD:41	inet addr:192.0.2.2
Bcast:192.0.2.20 Mask:255.255.255.0		
inet6 addr: fe80::201:d7ff:fe71:cd41/64 Scope:Link UP BROADCAST RUNNING MULTICAST MTU:4096 Metric:1		
RX packets:39088409 errors:0 dropped:0 overruns:0 frame:0 TX packets:37470798		
errors:0 dropped:0 overruns:0 carrier:0 collisions:0 txqueuelen:1000		
RX bytes:4141196638 (3949.3 Mb) TX bytes:694315251 (662.1 Mb)		
Interrupt:16		

The `clusterd` process controls the clustering technology for the VIPRION chassis. The `clusterd` process sends one multicast packet per second over the management backplane. If a blade fails to respond within 10 seconds, the `clusterd` process marks the blade down and logs an error message that appears similar to the following example to the `/var/log/ltm` file:

slot1/<hostname>	err clusterd[2346]: 013a0014:3: Blade 1: blade 4 FAILED
slot1/<hostname>	err clusterd[2346]: 013a0014:3: Blade 1: blade 4 FAILED
slot3/<hostname>	err clusterd[2365]: 013a0014:3: Blade 3: blade 4 FAILED



A blade can be logged as failed by another blade due to any factor that prevents the generation, transmission, or reception of the clusterd process packets. For example, a backplane hardware issue, congestion on the backplane, and excessive memory or CPU utilization on the sending blade can all potentially impede the clusterd process from processing clustering traffic in a timely manner.

VIPRION-specific SNMP traps

Other than normal alerts on the BIG-IP system, the traps that follow are specific to the VIPRION platform:

- bigipBladeTempHigh (“Blade temperature is too high.”)

```
BIGIP _ SYSTEM _ CHECK _ E _ BLADE _ TEMP _ HIGH _ 1 snmptrap OID=".1.3.6.1.4.1.3
375.2.4.0.87"
```

- bigipLibhalBladePoweredOff («Blade is about to be powered off.»)

```
BIGIP _ LIBHAL _ HALERR _ BLADE _ POWERED _ OFF snmptrap OID=".1.3.6.1.4.1.3375
.2.4.0.119"
```

- bigipBladeNoPower “A blade lost power. The blade may be pulled out”

```
BIGIP _ CLUSTERD _ CLUSTERD _ ERR _ BLADE _ PWRDOWN snmptrap OID=".1.3.6.1.4.1.
3375.2.4.0.88"
```

- bigipClusterdNoResponse “The cluster daemon failed to respond for 10 or more seconds.”

```
BIGIP _ CLUSTERD _ CLUSTERD _ FAILED snmptrap OID=".1.3.6.1.4.1.3375.2.4.0.89"
BIGIP _ CLUSTERD _ CLUSTERD _ TURNED _ RED snmptrap OID=".1.3.6.1.4.1.3375.2.4.0
.90"
```



Procedures

This section details how to do the following VIPRION-related tasks:

To find the right platform guide for your VIPRION system

1. Locate the product name on the front of your VIPRION chassis.
2. Go to [AskF5](#) and search for the string: “VIPRION <chassis_product_name> Platform Guide” (“VIPRION 2400 Platform Guide,” for example).

To add management IP addresses using the Configuration utility

1. Go to **System > Clusters > Management IP Addresses**.
2. Add management IP addresses for each slot in the **Cluster Member IP Addresses** area, and click **Update**.

To add management IP addresses using tmsh at the command line

1. Log in to the Traffic Management Shell (tmsh) by typing the following command:

```
tmsh
```

2. At the command prompt, type the following syntax:

```
modify /sys cluster default members { <slot#> ( address <IP address> } }
```

Replace **<slot#>** with the number of each slot contained on the VIPRION and **<IP address>** with assigned management IP address.

For example, to add **10.10.10.10** as the management IP address for slot1 type the following command:

```
modify /sys cluster default members { 1 { address 10.10.10.10 } }
```

3. Repeat step 2 for each slot number.
4. Save the configuration by typing the following command:

```
save /sys config
```

To configure multicast network failover using the Configuration utility

1. Under **Device Management**, click **Devices**.
2. Click the local hostname (the device labeled “**Self**”).
3. Under **Device Connectivity**, select **Failover Network**.
4. Under **Failover Multicast Configuration**, in Use **Failover Multicast Address**, select **Enabled**.
5. Review **Multicast Address**.



- Click **Update**.

To determine the primary blade on a VIPRION system using tmsh at the command line

- Log in to the Traffic Management Shell (tmsh) by typing the following command:

```
tmsh
```

- Type the following the command:

```
show /sys cluster
```

In the following sample output, the blade in slot 2 (172.24.62.132) is the primary blade, as shown in the Primary Slot ID entry.

```
-----
Sys::Cluster: default
-----
Address 192.0.2.0/24 Availability available State enabled
Reason Cluster Enabled Primary Slot ID 2 Primary Selection Time
1393007920
-----
| Sys::Cluster Members
+-----+
| ID   Address   Availability   State   Licensed   HA     Clusterd
Reason |
+-----+
| 1    192.0.2.1  available    enabled  true       active running
Run    |
| 2    192.0.2.2  available    enabled  true       active running
Run    |
| 3    192.0.2.3  available    enabled  true       active running
Run    |
| 4    192.0.2.4  available    enabled  true       active running
Run    |
+-----+
```

Shut down and reboot VIPRION systems at the command line

On a VIPRION system, the **reboot**, **halt**, **full_box_reboot**, and **shutdown** commands only affect the blade on which the command is executed. To execute a command on all available (green) blades, you can use the **clsh** command.

To shutdown command on all VIPRION blades

- At the command prompt, type:

```
clsh shutdown -r now
```




You can also shut down or reboot all blades with tmsh by specifying **slot all** with the required command.

To reboot all VIPRION blades

- At the command prompt, type:

```
tmsh reboot slot all
```

To reboot a specific slot

- At the command prompt, type:

```
tmsh reboot slot <slot number>
```

To view which blades are available

- At the command prompt, type:

```
tmsh show /sys cluster
```

When running the **shutdown** command, you can also use the **-k** flag to verify which blades will execute the command without shutting down or rebooting the system. For example:

```
[root@VIP-R22-S35:/Sl-P:Active] config # clsh shutdown -r -k now=== slot 2
addr 192.0.2.2 color green |
=== Shutdown cancelled.=== slot 3 addr
127.3.0.3 color green ===
Shutdown cancelled.=== slot 4 addr 192.0.2.4 color green === Shutdown
cancelled.=== slot 1 addr
127.3.0.1 color green === Broadcast message from root (Wed Mar 24 06:37:42
2015):
The system is going down for reboot NOW!
Shutdown cancelled.
```

```
[root@VIP-R22-S35:/Sl-P:Active] config #
```

If you want to execute the command in a specific order, you can use a “for” loop.

For example, to issue the **shutdown** command in the order of blade 1, 4, 2, 3, type the following command:

```
for i in 1 4 2 3 ; do echo "Running shutdown in slot
$i" ; ssh slot$i shutdown -r now ; done

[root@VIP-R22-S35:/Sl-P:Active] config # for i in 1 4
2 3 ; do echo "Running shutdown in slot $i" ; ssh slot$i shutdown -r now
; done
Running shutdown in slot 1
Broadcast message from root (Wed Mar 24 06:49:32 2015):
The system is going down for reboot NOW!
```



```
Running shutdown in slot 4
Running shutdown in slot 2
Running shutdown in slot 3
[root@VIP-R22-S35:/Sl- P:INOPERATIVE] config #
```

Replace a VIPRION chassis that has one or more blades installed

When you replace an existing VIPRION chassis that has one or more blades installed by moving the blades to a new chassis, you may experience the following issues:

- **Missing license:** When a blade is started up on a VIPRION chassis, the blade compares the serial number of the chassis on which it is currently running with the serial number recorded in its license file. If the serial numbers are different, the blade runs with no license, instead of using its existing license file.
- **Missing cluster configuration:** When a blade is started up on a VIPRION chassis, the blade compares the serial number of the chassis it is currently running on with its copy of the `/shared/db/cluster.conf.<chassis SN>` file. If the serial numbers are different, the blade runs with a factory-default cluster configuration instead of copying the `/shared/db/cluster.conf.<chassis SN>` file to the `/shared/db/cluster.conf` file, and using that as its cluster configuration. The `cluster.conf` file is made up of each blade's copy of the cluster configuration, the management addresses for the cluster, and each blade within the cluster, as well as other cluster-specific information.
- **Failure to load a configuration with SSL profiles that use the SSL key passphrase encryption:** If the VIPRION system or a vCMP guest that runs on the VIPRION system is configured with SSL profiles that use the SSL key passphrase encryption, moving the blades to a new chassis during a configuration load may result in SSL key passphrase errors.

If a UCS archive file is originally taken from a vCMP guest running on a blade and is reinstalled to the same vCMP guest running on the same blade, but inserted into a different chassis, the vCMP guest fails to load its configuration and reports an error message to the `/var/log/ltm` file.

For complete documentation on the chassis replacement procedure and its additional preventive maintenance tasks, see AskF5 article: [SOL14302: Replacing a VIPRION chassis that has one or more blades installed.](#)

Add a new blade to a cluster and monitor its status

Many changes to the VIPRION platform, such as adding a new blade, can take a long time to complete. To physically install a blade in a VIPRION chassis, follow the instructions in the appropriate platform guide for the hardware. The following sections are intended to provide assistance in monitoring the status of a newly installed blade as it becomes a member of the cluster.

Description

The slots in a VIPRION chassis work together as a single, powerful unit called a cluster. The size of the cluster depends on the number of running blades installed in the chassis.

When a blade is installed in a slot and is turned on, the blade automatically becomes a member of the cluster. For the newly installed blade to become a member of a cluster, the following automated events occur without user interaction:



- The system boots the newly inserted blade.
- The system copies software images from the primary blade to the newly inserted blade.
- The system installs software images on the newly inserted blade to match the boot locations of the primary blade.
- The newly inserted blade reboots to complete the software installation.
- The system may reboot the newly inserted blade an additional time to update the firmware.
- The system activates the newly inserted blade's license.
- The system places the newly inserted blade online and it becomes active.

These steps take time, and some of them may be repeated. For example, multiple reboots may be required when adding a blade with software installed in multiple boot locations. Make sure to plan enough time for the process.

1. The system boots the newly inserted blade

If you monitor the newly inserted blade using its console port, a login prompt displays when the system completes its initial boot. However, the blade is not yet an online or active member of the cluster. The system places the newly inserted blade into 'quorum' status.

You can view the status of the newly inserted blade at this time, using the **tmsh show /sys cluster** command on the primary blade.



The output of the command displays the quorum status, which appears similar to the following example:

```

-----
Sys::Cluster: default
-----
Address 192.0.2.0/24
Availability available
State enabled
Reason Cluster Enabled
Primary Slot ID 1
Primary Selection Time 0
-----
-----
| Sys::Cluster Members
| ID Address Availability State Licensed HA Clusterd
-----
+-----+
| ID Address Availability State Licensed HA Clusterd |
+-----+
| |1 192.0.2.2 available enabled true active running |
| |2 192.0.2.1 available enabled true active running |
| |3 192.0.2.3 unavailable enabled false active quorum |
| |4 : : unknown disabled false unknown shutdown |
+-----+

```

2. The system copies software images from the primary blade to the newly inserted blade

The system automatically copies software images from the primary blade to the newly inserted blade to ensure that the software images for each boot location match the other blades in the cluster.

You can use the **tmsk show /sys software status** command on the primary blade to determine if the newly inserted blade needs a software image from the primary blade. The command displays the “waiting for product image status” for each boot location needing a new software image.



The output of the command appears similar to the following example:

Sys::Software Status							
Volume	Slot	Product	Version	Build	Active	Status	
HD1.1	1	BIG-IP	11.1.0	1943.0	no	complete	
HD1.1	2	BIG-IP	11.1.0	1943.0	no	complete	
HD1.1	3	BIG-IP	11.1.0	1943.0	yes	complete	
HD1.2	1	BIG-IP	11.2.1	797.0	yes	complete	
HD1.2	2	BIG-IP	11.2.1	797.0	yes	complete	
HD1.2	3	BIG-IP	11.1.0	1943.0	no	waiting for	
						product image	
						(BIG-IP 1.2.1)	
HD1.3	1	BIG-IP	10.2.4	577.0	no	complete	
HD1.3	2	BIG-IP	10.2.4	577.0	no	complete	
HD1.3	3	BIG-IP	11.2.0	2446.0	no	waiting for	
						product image	
						(BIG-IP 10.2.4)	

No user interaction is required; the system automatically copies the software images from the primary blade. However, it may take several minutes for this to occur.

Ensure that you have software installation images and hotfix images available for each version of software that is installed into a boot location on the chassis.

For example, if you are running 11.3.0 HF1, and have 11.2.0 in another boot location, you should ensure that there are 11.3.0 and 11.2.0 installation ISOs as well as an 11.3.0 HF1 installation ISO available.

You can use the **tmsh list /sys software** command to see what installation images are available. If an installation image is missing, it can prevent the new blade from installing the appropriate software and becoming available.

3. The system installs software images on the newly inserted blade to match the boot locations of the primary blade

Once the software images are copied from the primary blade to the proper boot location of the newly installed blade, the installation of the software begins.

It is a good idea to have software installed in at least two boot locations. If software is only installed in one boot location, the



system can run into a deadlock condition trying to install software. For example, if the chassis only has boot location HD1.1 installed with version 11.4.0 software and you insert a blade, which only has boot location HD1.1 installed with version 11.3 software, the system cannot automatically install software to the new blade because it cannot install software to the active boot location.

You can monitor the status of the software installation using the **tmsh show sys software status** command on the primary blade. The command output indicates the installation completion percentage. The output of the command appears similar to the following example:

Sys::Software Status							
Volume	Slot	Product	Version	Build	Active	Status	
HD1.1	1	BIG-IP	11.1.0	1943.0	no	complete	
HD1.1	2	BIG-IP	11.1.0	1943.0	no	complete	
HD1.1	3	BIG-IP	11.1.0	1943.0	yes	complete	
HD1.2	1	BIG-IP	11.2.1	797.0	yes	complete	
HD1.2	2	BIG-IP	11.2.1	797.0	yes	complete	
HD1.2	3	BIG-IP	11.1.0	1943.0	no	waiting _ for _	
						productimage _	
						(BIG-IP _ 11.2.1)	
HD1.3	1	BIG-IP	10.2.4	577.0	no	complete	
HD1.3	2	BIG-IP	10.2.4	577.0	no	complete	
HD1.3	3	BIG-IP	10.2.4	577.0	no	installing _ 90.000	
						_ pct	

You can continue to monitor the status of the software installation by repeating the command on the primary blade.

Volume	Slot	Product	Version	Build	Active	Status	
HD1.1	1	BIG-IP	11.1.0	1943.0	no	complete	
HD1.1	2	BIG-IP	11.1.0	1943.0	no	complete	
HD1.1	3	BIG-IP	11.1.0	1943.0	yes	complete	
HD1.2	1	BIG-IP	11.2.1	797.0	yes	complete	
HD1.2	2	BIG-IP	11.2.1	797.0	no	complete	
HD1.2	3	BIG-IP	11.2.1	797.0	no	installing 10.000 pct	



	HD1.3	1	BIG-IP	10.2.4	577.0	no	complete	
	HD1.3	2	BIG-IP	10.2.4	577.0	no	complete	
	HD1.3	3	BIG-IP	10.2.4	577.0	no	complete	
+-----+								

4. The newly inserted blade reboots to complete the software installation.

Once the software installation is complete, the newly-inserted blade displays messages that appear similar to the following example, and then reboots:

```
slot3/VIP4400-R24-S42 emerg overdog[4097]: 01140043:0: Ha feature
software_update reboot requested. INIT: Switching to runlevel: 6
(reboot)

INIT: Sending processes the TERM signal INIT: Sending processes the KILL
signal Shutting down smartd: [ OK ]

Using bigstart to shutdown BIG-IP:
```

5. The system may reboot the newly inserted blade an additional time to update the firmware.

As the blade boots up following the software installation, it may require an additional reboot to update the firmware. If the firmware requires an update, the system displays messages that appear similar to the following on the blade's console:

```
Checking for firmware updates:

...

Updating HSB on mezzanine to version 1.4.2.0... DO NOT INTERRUPT Erasing
flash... (may take up to 30 secs)

Programming flash...

HSB firmware update: the system will automatically reboot to activate
slot 1. Updating HSB on main to version 1.4.2.0... DO NOT INTERRUPT

Erasing flash... (may take up to 30 secs) Programming flash...

HSB firmware update: the system will automatically reboot to activate
slot 1. INIT: Sending processes the TERM signal

Using bigstart to shutdown BIG-IP:
```

Following reboot, the blade boots to the same active boot location as the primary blade. As the blade boots back up following the firmware update, the system displays messages that appear similar to the following, to the blade's console:

```
Checking for firmware updates:

...

Successful update to HSB v1.4.2.0 Successful update to HSB v1.4.2.0
```

6. The system activates the newly inserted blade's license.

Once the blade has finished the required reboots, the system automatically activates the new blade's license. You can verify that the blade's license has been activated using the **tmsh show sys cluster** command on the primary blade. The Licensed column



in the output of the command shows a status of true for the newly inserted blade. The output of the command appears similar to the following example:

Sys::Cluster: default							

Address 192.0.2.0/24							
Availability available							
State enabled							
Reason Cluster Enabled							
Primary Slot ID 1							
Primary Selection Time 0							

Sys::Cluster Members							

+-----+							
ID	Address	Availability	State	Licensed	HA	Clusterd	
-----+							
1	192.0.2.1	available	enabled	true	active	running	
2	192.0.2.3	available	enabled	true	active	running	
3	192.0.2.2	offline	enabled	true	offline	running	
4	:	unknown	disabled	false	unknown	shutdown	
+-----+							

7. The system places the newly inserted blade online and it becomes active.

A short time after the system activates the blade's license, the system places the blade online and it is active. You can verify that the blade is online and active using the **tmsh show sys cluster** command on the primary blade. The output of the command appears similar to the following example:

Sys::Cluster: default							

Address 192.0.22.0/24							
Availability available							
State enabled							
Reason Cluster Enabled							
Primary Slot ID 1							
Primary Selection Time 0							

Sys::Cluster Members						

+-----+						
ID	Address	Availability	State	Licensed	HA	Clusterd
+-----+						
1	192.0.2.6	available	enabled	true	active	running
2	192.0.2.7	available	enabled	true	active	running
3	192.0.2.8	available	enabled	true	active	running
4	::	unknown	disabled	false	unknown	shutdown
+-----+						



Note If you are running BIG-IP software version 12.0.0 or later, you can use the disk-firmware-update.pl script to update the firmware on storage drives, that is, hard disk drives (HDDs) or solid-state drives (SSDs), that are installed in a BIG-IP platform or VIPRION blade.

Additional resources

The following table points to additional resources you can visit to learn more about the concepts and areas mentioned in this chapter. You can find AskF5 solution articles and the right product manuals for your software version by searching [AskF5 \(support.f5.com\)](https://support.f5.com).

Table 5.3: Additional resources

For more information about	See
VIPRION blades rebooting.	SOL11843: After installing an additional VIPRION blade, the new blade may reboot continuously.
VIPRION blades failing to join a cluster.	SOL14255: The B4300 blade may fail to join the cluster and reboot continuously.
Installing on the VIPRION.	SOL10633: BIOS update may be required before installing BIG-IP version 10.1.0 or later on the VIPRION platform.
Configuring network failover for redundant VIPRIONS.	SOL13915: Configuring network failover for redundant VIPRION systems (11.x).
Installing on the VIPRION.	SOL10633: BIOS update may be required before installing BIG-IP version 10.1.0 or later on the VIPRION platform.
Configuring network failover for redundant VIPRIONS.	SOL13915: Configuring network failover for redundant VIPRION systems (11.x).
Firmware	Storage Drive Maintenance in BIG-IP LTM F5 Platforms: Essentials .

Help improve this guide

Please help F5 improve this guide by responding to a few questions about this chapter.

(Note: You must be viewing this document in Adobe Acrobat Reader or similar to use this form.)

Did this chapter answer all of your questions about the subject matter? Yes No

If not, what information should be included that is not? _____

Did you find any errors pertaining to subject matter in this chapter? Yes No

If yes, please describe the error: _____

If yes, please copy and paste the paragraph containing the error here: _____

Did you find non-subject-matter errors in this chapter (spelling, etc.)? Yes No

If yes, please describe the error: _____

If yes, please copy and paste the paragraph containing the error here: _____



Drive Maintenance

At a glance—Recommendations

F5 has identified the following drive maintenance recommendations:

- Prevent disk utilization issues.
- Prevent full root file systems.
- Perform disk space cleaning.
- Understand how SMART check works.
- Check remaining lifetime on solid state drives (SSDs).
- Monitor RAID.
- View pendsect reporting for BIG-IP v11.2.1 HF-8, BIG-IP v11.3.0 HF-6, and BIG-IP v11.4.0 systems to help identify drive failures.

Background

This section provides context for our recommended procedures in the form of overviews and supplemental information, including:

- Understand the LVM disk-formatting scheme.
- Identify symptoms of a full/near full disk.

Logical volume management disk-formatting scheme

The BIG-IP version 11.x system uses logical volume management (LVM) disk-formatting. LVM is an enhanced software image manager used for deploying logical storage on a physical storage device or devices. Logical volumes may span across one or more physical hard drives and can be resized without interrupting service.

The BIG-IP LVM volume sets are formatted such that every product module includes a description of the file systems it needs, including a mount point and size for each volume. During installation, the BIG-IP system automatically allocates an appropriate amount of disk space when creating a volume set. In addition, the system allocates a certain amount of disk space for the shared volume, and the log volume.

Symptoms of a full/nearly full disk

When the BIG-IP file systems become full, undesirable or unpredictable behavior may result. Symptoms of a full or nearly full disk may include warning messages and/or traps from the diskmonitor utility or Daemon log messages.



Diskmonitor utility messages

The diskmonitor utility is a script that runs periodically on the BIG-IP system and alerts you if the partition space or volumes reach a defined threshold. If one or more of these thresholds are reached, a log message is logged to the `/var/log/ltm` file.

For example, the following message indicates that the **/shared** partition has less than 30 percent free space available:

```
diskmonitor: 011d005: Disk partition shared has less than 30% free
```

The following message indicates that the **/shared** partition has 0 percent free space available:

```
diskmonitor: 011d004: Disk partition shared has only 0% free
```

The following message indicates that the **/shared** partition is growing quickly:

```
diskmonitor: 011d004: Disk partition shared exceeded growth limit 10%
```

In addition, the BIG-IP system sends the following SNMP trap alerts when the partition space reaches a defined threshold:

bigipDiskPartitionWarn ("The disk partition free space is very limited, which is less than a specified limit. By default, the limit is set to 30% of total disk space.")

```
alert BIGIP _DMON _ERR _DMON _ALERT { snmptrap OID=".1.3.6.1.4.1.3375.2.4.0.25"}
```

```
alert BIGIP _DMON _ERR _DMON _WARN { snmptrap OID=".1.3.6.1.4.1.3375.2.4.0.25"}
```

bigipDiskPartitionGrowth "The disk partition exceeds the specified growth limit. By default, the limit is set to 5% of the total disk space. The growth is difference of two consecutive monitoring data."

```
alert BIGIP _DMON _ERR _DMON _GROWTH { snmptrap OID=".1.3.6.1.4.1.3375.2.4.0.26"}
```

Daemon log messages

If your disk is full or nearly full, Daemon log messages may appear similar to the following example:

```
Couldn't write to <file> / <partition> Failed to open file
```

The system performance may degrade, and you may see symptoms such as slow or failed disk writes. You may be unable to sync configurations or save a UCS file.

File storage

This section provides guidelines for optimal disk maintenance.

Store maintenance-related files

To help prevent disk usage issues, F5 recommends maintaining adequate disk space on the system:

- Store maintenance-related files in the **/shared/tmp** directory.



Maintenance-related files are those files that an administrator may create while doing maintenance or troubleshooting-related tasks on the system.

For example, tcpdump files, UCS archives, or qkview output files should be stored in the **/shared/tmp** directory.

Using the **/shared/tmp** directory for maintenance-related files is recommended for the following reasons:

- The BIG-IP installer allocates a large amount of disk space to the **/shared** partition.
- The **/shared/tmp** directory is shared between all installed images on a system. For example, if you save a tcpdump file to the **/shared/tmp** directory, each installation image or volume set has access to the tcpdump file.

Store long-term maintenance files on a network share. If you create files that are suitable for longer-term storage such as UCS archives or SCFs, F5 recommends moving them to a network share.

When creating or generating a file on the BIG-IP system, provide the full path location so that the file is saved to the intended location and not the current working directory.

For example, the following tcpdump command saves the capture file to the **/shared/tmp** directory:

```
tcpdump -ni1.1 -w /shared/tmp/example-tcpdump.pcap
```

The following qkview commands save the corresponding support file to the **/shared/tmp** directory:

```
qkview -f /shared/tmp/example-qkview.tar.gz
```

The following tmsh command saves the corresponding UCS file to the **/shared/tmp** directory:

```
tmsh save /sys ucs no-private-key /shared/tmp/example- config.ucs
```

Avoid storing files in directories that reside on the root filesystem. The BIG-IP system has a relatively small root filesystem, and separate partitions for filesystems, such as **/config**, **/usr**, and **/shared**. Directories, such as **/home** reside on the root filesystem and should not be used for file storage.

Store image files in **/shared/images/**. If you upload installation images to the BIG-IP system using the command line, you should store them in the **/shared/images** directory. As you remove old images, removing the old files in **/shared/images** will avoid filling this partition.

Check available disk space

To check available disk space, you can type the **df -h** command. For example, the following **df -h** output indicates that the root file system is at 100 percent usage:

Filesystem	Size	Used	Avail	Use%	Mounted on
/dev/mapper/vgdbdsaset.1.root	380M	214M	147M	60%	/
/dev/mapper/vgdbdsaset.1.config	3.0G	77M	2.8G	3%	/config
/dev/mapper/vgdbdsaset.1._usr	2.7G	2.0G	643M	76%	/usr



/dev/mapper/vgdbdsdataset.1. _var	3.0G	415M	2.4G	15%	/var
/dev/mapper/vgdbdsadat.share.1	20G	269M	19G	2%	/shared
/dev/mapper/vgdbdsadat.log.1	485M	32M	428M	7%	/var/log
none	2.0G	956K	2.0G	1%	/dev/shm
none	2.0G	30M	2.0G	2%	/shared/rrd.1.2
none	2.0G	5.5M	2.0G	1%	/var/tmstat
none	2.0G	1.2M	2.0G	1%	/var/run
prompt	4.0M	28K	4.0M	1%	/var/prompt
none	2.0G	0	2.0G	0%	/var/loipc

Periodically check the inode usage on the BIG-IP system. To check inode usage, run the **df -i** command. For example, the following **df -i** output indicates the **/var** filesystem has no free inodes:

df-i	Filesystem	Inodes	IUsed	IFree	IUsed%	Mounted on
	/dev/md	765536	3384	62152	6%	/
	/dev/md9	393216	307	392909	1%	/config
	/dev/md8	219520	28044	191476	13%	/usr
	/dev/md10	393216	393216	0	100%	/var
	/dev/md0	3932160	200	3931960	1%	/shared
	/dev/md1	917501	159	917345	1%	/var/log
	none	1023877	39	1023838	1%	/dev/shm
	none	1023877	27	1023850	1%	/var/tmstat
	none	1023877	182	1023895	1%	/var/run
	prompt	1023877	4	1023873	1%	/var/prompt
	/dev/md15	1572861	188	1572676	1%	/var/lib/mysql

If inode usage is at or near 100 percent, move any unnecessary maintenance-related files from the BIG-IP system to a network share and schedule a time to reboot the system.

Periodically check for and remove non-critical maintenance files.

In many cases, non-critical maintenance files will be apparent and can be safely removed. For example, old tcpdump, qkviews, or core files should be deleted from the system or moved to a network share. You can use the find command to locate old maintenance-related files. For example, to locate the 20 largest files on the system, you would type the following command syntax:

```
find <dir> -xdev -type f | xargs du | sort -rn | head -20
```

For example, the find command below was used to locate the 20 largest files in the **/shared** partition, some of which can be safely removed, such as the 2 GB tcpdump file, and the 18 MB core file:

```
find /shared/ -xdev -type f | xargs du | sort -rn | head -20 2189582 /
shared/tcpdump.cap 1277060
/shared/images/BIGIP-11.3.0.2806.0.iso 1186512 /shared/images/BIGIP-
11.2.1.797.0.iso
```



18460	/shared/core/mcpd.bld3341.0.core.gz
5200	/shared/rrd.1.2/endpiession
4984	/shared/rrd.1.2/blade0cpu
3796	/shared/bin/big3d
2460	/shared/rrd.1.2/connections
1308	/shared/rrd.1.2/throughput
1164	/shared/rrd.1.2/memory
1096	/shared/rrd.1.2/rollupcpu
876	/shared/rrd.1.2/gtm
732	/shared/rrd.1.2/ramcache
588	/shared/rrd.1.2/bwgain
224	/shared/tmp/packages/rt.pkc
156	/shared/rrd.1.2/bladeconnections
48	/shared/tmp/packages/tmui.pkc
20	/shared/tmp/packages/schema.pkc
16	/shared/tmp/packages/axis.pkc
12	/shared/tmp/packages/packages.idx
12	/shared/rrd.1.2/endpiession.info
12	/shared/rrd.1.2/blade0cpu.info

Diskmonitor utility

The diskmonitor utility is a script that runs periodically on the BIG-IP system to monitor disk use. The diskmonitor utility does the following functions:

- Monitors BIG-IP system disk usage limits and disk usage growth rates on selected partitions.
- Sends warning and error logs to syslog when partitions are running out of space.
- Dynamically adjusts the diskmonitor utility, which is executed when disk use is approaching critical levels.

The following partitions are monitored, by default:

root	=	/
config	=	/config dev _ shm = /dev/shm
shared	=	/shared usr = /usr
var	=	/var
var_log	=	/var/log var_run = /var/run



Configuration variables for the diskmonitor utility

The db variables allow customization of the diskmonitor utility on a per partition basis, as well as the option to disable the diskmonitor utility.

Logging warning and error conditions

The diskmonitor utility reports error and warning conditions to the syslog-ng utility. For details about each error and warning condition, see the following table:

Table 6.2: Logging and error conditions

Error or warning condition	Message number	Message report	Description
syslog-ng<logfacility>.<severity level>: local0.error	011d0002	No diskmonitor entries in database.	The bigpipe db utility cannot find any Platform. DiskMonitor db keys.
syslog-ng<logfacility>.<severity level>: local0.warning	011d0002	Cannot access the database because mcpd is not running.	The mcpd process needs to be running for diskmonitor to get its db key configuration.
syslog-ng<logfacility>.<severity level>: local0.warning	011d0003	Error parsing df -k output.	The diskmonitor utility could not get the free space percentage from df -k.
syslog-ng<logfacility>.<severity level>: local0.error	011d0004	Disk partition <partition> has only <percentage> free.	The monitored partition<partition> has only a critical amount of free space left.
syslog-ng<logfacility>.<severity level>: local0.warning	011d0005	Disk partition <partition> has only <percentage> free.	The diskmonitor utility sends a warning message because the monitored partition has less free space remaining than the warning level specifies.
syslog-ng<logfacility>.<severity level>: local0.warning	011d0006	Disk partition <partition> exceeded growth limit <growth percentage>.	The diskmonitor utility detects that the usage in the monitored partition is growing quickly (the usage exceeded the growth percentage after its last monitored interval).



Procedures

This section describes maintenance tasks to be done on a regular schedule or in response to monitoring findings, including:

Monitor RAID

Some F5 devices—notably the 6900, 8900, and 8950—have two redundant disks set up in a RAID array. The RAID array can be degraded if there is a problem with one of the disks. This section describes how to monitor your system to be certain the RAID system has both disks participating, and information on repair if you need to replace a disk.

Manage log files on the BIG-IP system

The following prerequisites are necessary to manage log files:

- You must have command-line access to the BIG-IP system.
- You should have familiarity with using a Linux text editor.

You can configure the following log-related elements on the BIG-IP system:

- Change the log rotation frequency.
- Change the age at which log files become eligible for removal.
- Change the number of archive copies that the system retains
- Add a custom option to the log rotation process.

Prevent full file systems

Store scratch data in the shared partition: Any scratch data, is data you want to stage for deployment on or retrieve from the BIG-IP system should be stored in the **/shared** partition. This includes troubleshooting data. Ideally, you would want to store all scratch data off the BIG-IP system by using a central repository such as CVS or Git, but if you cannot do that, the shared partition is the best option because data placed here is visible and shareable.

For more information, see [Manage log files on the BIG-IP system](#) and [Causes of excessive logging](#).

Perform disk space cleaning

Monitoring the hard disk capacity on a BIG-IP system is critical to maintaining its health. If a BIG-IP system is running low on disk space, you may experience performance-related issues, such as the inability to do upgrades, run ConfigSync operations, or save UCS files.

F5 recommends periodically checking disk space and taking action when you reach a threshold defined by your processes and procedures.



SMART check your disks

Self-Monitoring, Analysis, and Reporting Technology (SMART) checks should not generally be necessary on BIG-IP v10.2.4 HF-7, BIG-IP v11.2.1 HF-8, BIG-IP v11.3.0 HF-6, and BIG-IP v11.4.0 and later.

Additionally, a SMART test is run as part of the EUD process recommended on an annual basis.

SMART helps to detect indications the disk is likely to fail. At BIG-IP v11.2.1 HF-8, BIG-IP v11.3.0 HF-6, and BIG-IP v11.4.0, the `pendsect` utility will detect SMART errors on most platforms, and produce logging that recommends action, including running SMART through EUD.

In BIG-IP v11.4.0 and later, you can also use the **platform_check** command to collect the SMART test data from the drive. The disk portion of the command output indicates a Pass or Fail status for the drive and logs detailed information to the **/var/log/platform_check** file.

SMART check SSDs

SMART checks can be used on your SSDs as well. This is a command-line method to get to the same information that is available through the Configuration utility.

A SMART test is run as part of the EUD process recommended on an annual basis.

The only valid SMART attribute for SSDs is the Media Wearout Indicator.

To run SMART check on SSDs using `tmsh` at the command line

1. Determine the disk drives you have in your system.
2. Log in to the Traffic Management Shell (`tmsh`) by typing the following command:

```
tmsh
```

3. At the command prompt, type:

```
run util bash fdisk -l
```

To determine the name of your SSD at the command line

- At the command prompt, type:

```
smartctl -a /dev/sda | grep 233
```

The returned result will appear similar to the following:

```
233 Media_Wearout_Indicator 0x0032 100 100 000 Old_age Always - 0
```

The code 233 indicates the attribute number of the **Media_Wearout_Indicator**.

The hex value 0x0032 is a flag and is unimportant for this analysis. The following number will be the value from 0 to 100. A value of 100 indicates 100 percent of the disk life remains; a value of 0 indicates that the disk has reached



the maximum number of writes expected from the drive.

TRIM

Solid-state drives (SSDs) should have TRIM support turned on. TRIM is set up by default on F5 systems that include SSDs. TRIM support slightly reduces the amount of space available on your SSD, and improves its performance by keeping pages available as the memory on the SSD is overwritten. It will operate automatically and should not interfere with the amount of space available for data.

Check remaining write lifetime on SSDs

If you are using SSDs for datastore on the 11000 or 11050 systems, or are using SSDs for main storage for new appliances, you can view the SSD allocation and monitor the SSD lifespan.

To view the SSD allocation and monitor the SSD lifespan using the Configuration utility

1. Under System, click **Disk Management**.
2. View details about the SSDs, including the following:
 - To view the general properties of a disk, in the **Logical View** area, click **disk label**.
 - In the **Physical View** area, note which bays contain the SSDs.
 - In the **Data Disks** area, view the **Media Wearout Indicator** to monitor disk usage.

Monitor RAID status

There are four ways to receive monitoring data for RAID status on a BIG-IP system:

- The Configuration utility notes that the RAID status is degraded if one of the disks is offline.
- BIG-IP iHealth displays an error at the top of your page if you view a qkview where one of the two disks in a RAID array is offline.
- tmsh allows you to view RAID status by typing the following command:

```
showsysraidarray
```

- Syslogs can be searched for the following phrase:

```
alert kernel: raid1: Disk failure
```

If there are any results of this search, it will tell you which disk has had a problem.

If any of these methods show a degraded RAID status, you should contact F5 Technical Support as it will most likely need be necessary to replace a disk.



Repair disk errors on BIG-IP systems with RAID storage

If both disks show data loss or you suspect other issues, contact F5 Technical Support for assistance.

If you have a replacement disk from F5 and need to rebuild your RAID array, see the appropriate platform guide for your hardware platform.

For more information on repairing disk errors, see Ask F5 article: [SOL12756: Repairing disk errors on RAID-capable BIG-IP platforms](#).



Note The RAID system on an F5 system must have the old disk explicitly removed from the array and the new disk added manually before the new disk is operational.

View pendsect reporting to help identify actual drive failures

At BIG-IP v11.2.1 HF-8, BIG-IP v11.3.0 HF-6, and BIG-IP v11.4.0, the pendsect feature of TMOS helps improve disk error detection, correction, and messaging on the drives in the following:

- 1600
- 3600
- 3900
- 6900
- 8800
- 8900
- 8950
- 11000
- 11050
- 2000
- 4000
- 5000
- B4100 blades with 160Gb drives,
- B4200
- B4300



- B2100
- B2150

The pendsect utility helps you identify actual drive failures and reduce the number of unnecessary return material authorizations (RMAs) your operations center processes. The software periodically checks for pending sector alerts and resolves them. It is configured to run daily and provides improved disk error detection and correction. The system logs the pendsect messages to the **/var/log/user.log** file. When the pendsect process runs and no errors are detected or corrected, the system logs messages that appear similar to the following example:

```
warning pendsect[21788]: pendsect: /dev/sdb no Pending Sectors detected
```

When the pendsect process detects and corrects an error, the system logs messages that appear similar to the following example:

```
warning pendsect[19772]: Recovered LBA:230000007
```

```
warning pendsect[19772]: Drive /dev/sda partition UNKNOWN warning  
pendsect[19772]: File affected NONE
```

When the pendsect process detects an error and is unable to correct the error, the system logs messages that appear similar to the following example:

```
warning pendsect[20702]: seek(1) error[25] recovery of LBA:226300793 not  
complete warning pendsect[20702]: Drive: /dev/sda filesystem type:
```

```
Undetermined warning pendsect[20702]: File affected: NONE
```

If pendsect reports an error, you cannot correct, or if you suspect a possible disk failure, you can do the End-User Diagnostic (EUD) SMART test to test the drive.

fsck utility

The fsck utility runs automatically on reboot so it does not require being run by an administrator on BIG-IP units.

Additional resources

The following table points to additional resources you can visit to learn more about the concepts and areas mentioned in this chapter. You can find AskF5 solution articles and the right product manuals for your software version by searching [AskF5 \(support.f5.com\)](https://support.f5.com).



Table 6.3: Additional resources

For more information about	See
Pendsect.	SOL14426: Hard disk error detection and correction improvements (versions 11.4.1, 11.4.0, 11.3.0, 11.2.1, and 10.2.4).
RAID Status degraded after a hard drive replacement.	SOL12380: RAID capable BIG-IP platforms report the RAID status as degraded in the Configuration utility after a hard drive replacement (versions 11.4.1, 11.4.0, 11.3.0, 11.2.1, 11.2.0, 11.1.0, and 11.0.0).
Reboot loop upon disk replacement.	SOL13654: Replacing a disk may cause a reboot loop on BIG-IP 6900, 8900, or 8950 platforms (versions 11.4.1, 11.4.0, 11.3.0, 11.2.1, 11.2.0, 11.1.0, and 11.0.0).
Repairable disk errors.	SOL12756: Repairing disk errors on RAID-capable BIG-IP platforms (versions: 11.5.0, 11.4.1, 11.4.0, 11.3.0, 11.2.1, 11.2.0, 11.1.0, and 11.0.0).
Upgrading to 11.0 or 11.1 without using RAID.	SOL11965: Disabling RAID drive mirroring (versions 11.1.0 and 11.0.0).
Modifying a system with an undefined RAID array.	SOL14269: Attempting to modify an undefined RAID array may result in error or an unexpected format of the hard drive (versions 11.3.0, 11.2.1, 11.2.0, 11.1.0, and 11.0.0).
Replacing the hard drive.	<i>Platform Maintenance</i> in the appropriate Platform Guide for your system. See Additional Resources in the VIPRION chapter (versions 11.5.0, 11.4.1, 11.4.0, 11.3.0, 11.2.1, 11.2.0, 11.1.0, and 11.0.0).

Help improve this guide

Please help F5 improve this guide by responding to a few questions about this chapter.

(Note: You must be viewing this document in Adobe Acrobat Reader or similar to use this form.)

Did this chapter answer all of your questions about the subject matter? Yes No

If not, what information should be included that is not? _____

Did you find any errors pertaining to subject matter in this chapter? Yes No

If yes, please describe the error: _____

If yes, please copy and paste the paragraph containing the error here: _____

Did you find non-subject-matter errors in this chapter (spelling, etc.)? Yes No

If yes, please describe the error: _____

If yes, please copy and paste the paragraph containing the error here: _____



BIG-IP Virtual Edition

At a glance—Recommendations

F5 has identified the following cloud environment recommendations:

- Set up BIG-IP VE for Cloud: Microsoft Azure.

Background

BIG-IP VE for Cloud: Microsoft Azure

BIG-IP VE v. 12 and higher support Microsoft Azure cloud-based environment. There are significant differences between Azure and other cloud environments, and F5 strongly encourages users to become familiar with the information in this section before running BIG-IP VE in the Azure cloud.

Microsoft Azure supports BIG-IP modules AFM, APM, LTM, AM, ASM, and DNS (formerly GTM).

BIG-IQ and EM

Neither BIG-IQ nor EM are not currently supported in Azure.

Restore default configuration

Restoration of default configuration is not supported in Azure.

While standard environments allow you to run the **tmsh load sys config default** command to reset the BIG-IP to default configuration, this is not possible in Azure. If you attempt this, BIG-IP will error out when it attempts to reset the management and self IP addresses.

If you need to return to default configuration, create a new instance of BIG-IP instead.

For more information, see Ask F5 article [SQL17463: The BIG-IP Virtual Edition may fail to load the default configuration on the Microsoft Azure cloud service](#) and the [BIG-IP Virtual Edition Setup Guide for Microsoft Azure](#).

Azure environment

Azure uses a modified version of the Hyper-V hypervisor from Microsoft as the cloud platform. Because it is a modified version, virtual machines (VMs) running on Hyper-V may not necessarily run on Azure. The URL for Azure is **<https://portal.azure.com>** and a user needs a Windows Live account ID to log in.

Azure uses cloud services as an isolation of a private cloud environment, similar to the virtual private cloud (VPC) concept in Amazon Web Service (AWS). However, unlike AWS, which requires a VPC to be created before provisioning a virtual machine into it, Azure can also have cloud services created with the VM creation.

There is no need to define subnets in Azure for your VM implementation; Azure Fabric automatically assigns one (and only one



NIC) along with a private, non-routable IP to a VM. There will also be a public IP assigned for the VM (not to a VM) on the Azure portal. The IP address on the VM is non-routable and you need to set up the inbound rules at the network security group (NSG) to map the services port on the public IP to the private non-routable IP.

Similar to Amazon AWS, Azure doesn't provide console access to the VM. Access will be limited to ssh or other services the VM can expose via the management interface, for example, http or https.

The MAC address for the VM does not persist across a shutdown or restart from Azure portal, with the reason being is that, when a VM is shutdown by Azure, all of the resources, including CPU, memory, and MAC address are deallocated.

Note that because the MAC address is not persistent after a shutdown/restart, the IP address a VM gets from DHCP also changes. Since both the internal and public IP address assigned change across a stop/restart, an admin has to config a DNS name for the VM so that it can be persistently accessed from outside.

Key differences between BIG-IP VE in Azure and BIG-IP VE in other environments include the following :

- BIG-IP VE uses only one network interface in the Azure cloud. This means that both MGMT and TMM share one interface.
- In most cases, BIG-IP VE will run in one-armed deployment in the Azure cloud.
- BIG-IP uses only one IP address in the Azure cloud. This means that MGMT IP, self IP, and virtual server IP all share one IP address. For example **10.20.0.0/16**.
- The preferred standard username/password combinations of **admin/admin** and **root/root** are not available in BIG-IP VE in the cloud.
- BIG-IP VE version 12.0 does not support Azure diagnostics.
- High-availability (HA) configuration is not supported in BIG-IP VE version 12.0.

Configure a virtual server in Microsoft Azure

When BIG-IP is booted, the MGMT interface is setup by DHCP. Additionally, Self IP VLAN and default gateway will automatically be configured by startup script.



Important SNAT must be enabled in your virtual server profile. It is disabled by default.

However, a new IP address will be assigned to BIG-IP every time it is rebooted. This means that when you set up a virtual server IP, the destination address will change. Therefore, you cannot configure a conventional destination IP address in the virtual server profile. You must instead set the wild card address: **0.0.0.0:80**.

This is a known issue that Microsoft is working to fix.



Warning Because BIG-IP has IP address automatically assigned, DO NOT try to set up a self IP or add second IP to the interface. It is allowed but you should not do it as your BIG-IP instance will be lost and require rebooting.

Root account and admin account setup

The preferred standard username/password combinations of **admin/admin** and **root/root** are not available in BIG-IP VE.

Further, you must set up a username and password for the administration account. These will be the credentials you use to log in to the BIG-IP VE system each time.

Root access is disabled on all cloud platforms for security.

Disable diagnostics

Azure does not currently support BIG-IP VE 12.0 diagnostics.



Important You must manually disable Diagnostics in the Monitoring section of Create virtual machine dialog before you will be able to deploy.

Skip high availability configuration

High availability configuration is not supported in this version of Microsoft Azure.



Important When you set up and license for the first time and resource provision, you will be asked to provide information such as hostname password, and so on. When you are prompted to set up HA configuration, you must skip this step or an error will occur.

DNS name

Because the IP address changes every time, to persist connection, have to setup DNS name for that BIG-IP. By default it is not set up. Set up on Azure cloud side not BIG-IP.

Assignment of a DNS name to a virtual machine/application for persistent access needs to be done after a virtual machine is already provisioned and running. You will need to manually configure the DNS name field. It is not set up by default.

The full DNS name should reflect the region where the VM is located. For example: **mybigip.eastus2.cloudapp.azure.com**. In this example, “**eastus2**” would indicate that the virtual machine is located in US east region 2.



If you plan to use your own DNS name, you can create a CNAME record on your own authorized DNS server and map it to the Azure DNS name. For example: **mybigip.useast2.cloudapp.azure.com** to **mybigipuseast2.azure.com**. In this example you would be able to access the virtual machine or application using the URL **mybigip.useast2.cloudapp.azure.com**.

Network Security Group setup

If you set up a virtual server at port 80, you will be unable to access that IP and port from outside because a firewall exists between BIG-IP and outside traffic. To pass traffic through the firewall, you need to set a rule or a policy on the Network Security Group to forward the traffic to a virtual machine.

Port offloading

In the Azure environment, management IP, self IP, and virtual server IP all share the same address and BIG-IP management service already uses ports 443 and 22. If you want to use ports 443 or 22 for server load balancing, you will first need to move the management services to other ports.

Procedures

To change the HTTPS port using tmsh at the command line

- Type the following command:

```
tmsh modify sys httpd ssl-port
```

To change the SSH port using tmsh at the command line

- Type the following command:

```
tmsh modify sys sshd port
```



Tip When moving the HTTPS and SSH ports from their default location, you must select port 1024 or higher.



Additional resources

The following table points to additional resources you can visit to learn more about the concepts and areas mentioned in this chapter. You can find AskF5 solution articles and the right product manuals for your software version by searching [AskF5 \(support.f5.com\)](https://support.f5.com).

Table 6.1: Additional resources

For more information about	See
Loading default configuration	SOL17463: The BIG-IP Virtual Edition may fail to load the default configuration on the Microsoft Azure cloud service
Microsoft Azure setup	BIG-IP Virtual Edition Setup Guide for Microsoft Azure
Microsoft Azure and BIG-IP	The BIG-IP Platform and Microsoft Azure: Application Services in the Cloud

Help improve this guide

Please help F5 improve this guide by responding to a few questions about this chapter.

(Note: You must be viewing this document in Adobe Acrobat Reader or similar to use this form.)

Did this chapter answer all of your questions about the subject matter? Yes No

If not, what information should be included that is not? _____

Did you find any errors pertaining to subject matter in this chapter? Yes No

If yes, please describe the error: _____

If yes, please copy and paste the paragraph containing the error here: _____

Did you find non-subject-matter errors in this chapter (spelling, etc.)? Yes No

If yes, please describe the error: _____

If yes, please copy and paste the paragraph containing the error here: _____



Licenses and Entitlement

At a glance—Recommendations

F5 has identified the following license and entitlement recommendations:

- Check for license expiration.
- Check that your licenses are valid.
- Schedule license renewals.

Background

This section provides context for our recommended procedures in the form of overviews and supplemental information, including information on the following topics:

- Licenses.
- Provision licensed modules.
- License Virtual Edition (VE) and appliances.

Licenses

When you purchase support from F5, it is associated with a particular BIG-IP system. A system with an active support contract is considered entitled until such time the contract expires. When a support contract expires, the system is not entitled to support until the contract is renewed.

Licenses are also associated with the modules you purchase to run on the system. These model licenses are an add-ons to the main license for your system. Add-on licenses are automatically linked to the main BIG-IP system license and eligible for technical support as long as that system is entitled.

Major software upgrades are only supported for entitled systems and require relicensing the BIG-IP system. Minor upgrades do not require relicensing.

F5 recommends checking your BIG-IP system entitlement every six months.

For more information, see AskF5 article: [SOL7752: Overview of licensing the BIG-IP system](#).

Licensed modules are not functional until provisioned

If you have installed a license for an add-on module on a BIG-IP system, it is necessary to provision resources for the add-on module.

Modules will experience the following limitations until provisioned:



- The system will not do the functions of the licensed module.
- Items related to the module will not appear in Configuration utility menus.
- The tmsh utility will not present or permit configuration of objects related to the module.
- The **bigstart status** command will return output similar to the following example for daemons related to the unprovisioned module:

```
<daemon _ name>down, Not provisioned
```

For information on provisioning modules, see [Provision licensed modules in your BIG-IP system](#).



Note In some versions, configuration objects related to unprovisioned modules are incorrectly exposed. For more information, see AskF5 article: [SOL10376: The Configuration utility allows configuration of unprovisioned modules](#).

When you upgrade a BIG-IP system, the install script verifies the service check date with the license check date of the version being installed. If the service check date is missing or the verification process finds your license pre-dates the software's release date, a line will display in the **/var/log/liveinstall.log** with a note about the service check date verification, and the installation of the software may continue.

Evaluation and subscription service licenses

Evaluation licenses and subscription service licenses granted by F5 have their own subscription service and expiration dates. When an evaluation license ends, the module becomes inactive and all configuration items are expected to cease functioning.

When a subscription period ends, the system service will no longer receive updates. In the case of the IP Intelligence service, the IP address database will become outdated.

The subscription-based feature is expected to continue functioning as designed, but with outdated data.

BIG-IP Application Security Manager attack signatures

BIG-IP Application Security Manager (ASM) attack signatures will not update if the Service Check Date is not within 18 months of the system date. BIG-IP ASM will attempt to update the service check date automatically. If it cannot reach the license server and the service check date is less than seven days from the system date, BIG-IP ASM will attempt an attack signature update anyway. After seven days from the system date, you may have to manually reactivate the system license and re-initiate the attack signature update.



Procedures

Follow the procedures detailed in this section to guide you in managing licenses and entitlement.

Reactivate a BIG-IP system license

Before you do a software upgrade, F5 recommends you reactivate BIG-IP system license.

To reactivate your BIG-IP system license using the Configuration utility

1. Go to **System > License**.
2. Click **Re-activate**.
3. In the **Activation Method** area, select **Automatic** (requires outbound connectivity).
4. Click **Next**.

The BIG-IP software license renews.

View and verify a BIG-IP system license

There may be occasions when you need to test the validity of the BIG-IP software license.

You can obtain license information in any of the following ways:

- From the command line.
- Request a product license profile from F5.
- View license profile in BIG-IP iHealth.
- View license profile in the Configuration utility.

To view license information at the command line

- At the command prompt, type:

```
tmsh show /sys license
```

Output displays licensing information for the BIG-IP system, including a list of active modules.

For a system with a valid license, output will appear similar to the following example:

```
Sys::License
Licensed Version 11.4.1
Registration key Txxxx-xxxxx-xxxxx-xxxxx-xxxxx26 Licensed On 2014/03/14
License Start Date 2014/03/13 License End Date 2014/04/14 Service Check
```




Date	2014/03/14	Platform ID
		Z100
Active Modules		
	ASM, 5Gbps, VE	(G536528-5957369)
	IPV6 Gateway Rate Shaping Ram Cache	
	50 Mbps Compression Client Authentication AFM, VE Routing Bundle, VE	PSM, VE

If your system license is not properly installed, basic system functionality is lost, and the tmsh command output does not show the active modules enabled on the system.

Output for a system with a missing license will appear similar to the following example:

```
Can't load license, may not be operational
```

To inspect the expiration date at the command line

- At the command prompt, type:

```
grep trust /config/bigip.license
```

The system will return an IP intelligence license key value that appears similar to the following example:

```
20120809 _subscr _trusted _i 290345338
```

The initial eight-digit response indicates the system license expiration date in YYYYMMDD format.

To check query the status of the IP Intelligence at the command line

- At the command prompt, type:

```
tmsh show sys iprep-status.
```

Output will return the following information:

- Date and time that the BIG-IP system last contacted the vendor server the date.
- Time that the BIG-IP system last received an update.
- Total number of IP addresses in the database.
- Number of IP addresses in the most recent update.

For more information, see AskF5 article: [SOL13776: Determining the IP intelligence subscription expiration date.](#)



Note Another subscription service you may want to monitor is the WhiteHat Sentinel web application vulnerability scanner. That subscription is managed on the Whitehat website. For more information, see AskF5 article: [SOL11926: Integrating BIG-IP ASM with WhiteHat Sentinel](#).

To request a product license profile from F5

1. Go to the F5 [Product Information Request](#) page (secure.f5.com/validate/validate.jsp)
2. Enter your contact email.
3. In the **F5 Licenses / Serial Numbers** field, type the serial number(s) or base registration key(s).
4. Click **Submit Info Request**.

A license summary for the entered registration keys will be sent to the email address you entered.



Note In BIG-IP v. 12 and higher, if you attempt to install a license that is not compatible, the system will warn you that the new license could cause a lack of functionality and ask you to confirm if the new license should be installed.



The email appears similar to the following example:

```

From: F5 Networks
Sent: Monday, January 1, 2015 12:34 AM To: John Doe
Subject: Information for F5 Keys
ABCDE-FGHIJ-KLMNO-PQRST-UVWXYZA
#-----#
# F5 License Information Server#
# Thank you for requesting a product license profile
# from F5 Networks. To better understand the information
# provided below, you may want to refer to the Product License
# Profile solution on AskF5 for definitions of the values included
# in the profile.#
#-----#
#-----#
F5 License Information for ABCDE-FGHIJ-KLMNO-PQRST-UVWXYZA
#-----#
Serial Number : bip012345s (D68)F5 Product
: F5-BIG-LTM-6800-E2 BIG-IP SWITCH:
LTM 6800 ENTERPRISE (4GB MEM, 2GBCMP,20KSSL,RS,Usage :ProductionEntitled
Service :
12-31-2014 - 12-31-2015 (F5-SVC-BIG-PRE-9)Warranty Date :12-31-2015
-----
Base Key for BIG-IP 9.x
-----
F5 Platform : D68
Activation Date : 12-31-2015
Base RegKey : UVWXYZA (Locked)
BIG-IP Mac Address : 00:01:a1:23:b0:45
Add-on: ABCDEFG (Active) BIG-IP LTM
Add-on : HIJKLMN(Active) BIG-IP LTM Enterprise 6800
#-----#
# Copyright © 1999-2015, F5 Networks, Inc.# All rights reserved.
#-----#

```



License information in BIG-IP iHealth

- If your system is nearing the end of support entitlement, a banner message will appear on the main **Status** page.

To inspect the expiration date using the Configuration utility

1. Go to **System > License**.

2. Locate the entry for the IPI Subscription module

The expiration date will be listed beneath the IPI Subscription entry, for example:

Subscription expires after Aug 9, 2015.

As the expiration date approaches, a banner warning will also display on the license page when you log in to the Configuration utility.

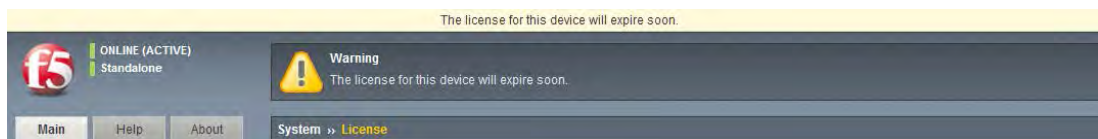
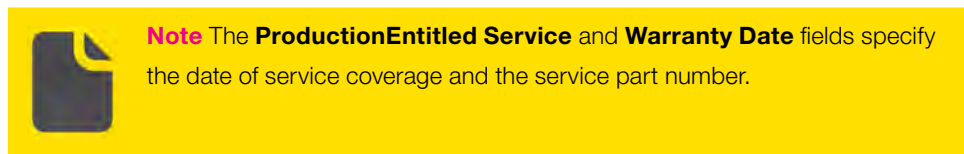


Figure 8.1: License expiration warning in Configuration utility

License the BIG-IP system

Before you can configure and use the BIG-IP system, you must activate a valid license on the system.

To license the BIG-IP system, you must do the following procedures:

- Obtain a registration key.
- Obtain a dossier.
- Activate the license.



Obtain a registration key



Before you can activate the license for the BIG-IP system, you must obtain a base registration key. The base registration key is a 27-character string that instructs the license server which F5 products you can license. The base registration key is pre-installed on new BIG-IP systems.

When you connect to the Configuration utility, the **Licensing** page displays the registration key.

The format of the BIG-IP base registration key is as follows:

AAAAA-BBBBB-CCCCC-DDDDD-EEEEEE

If you do not have a base registration key, contact your F5 Sales representative, or F5 Technical Support

Obtain a dossier

The dossier is an encrypted list of key characteristics used to identify the platform, which you can obtain from the BIG-IP software. It is generated by your F5 product after you choose a license activation method and will appear similar to the following truncated example:

```
e fe3bef1df38cb46ca4c1f82f6d03a02ea2d8da4d26767cb801c1e4b4024
08b1f763a09ff571ca860e4d61ebdb010ae8c86de7966c267436cbe27e
6d9900db229c2b96ddc4bf48c54cd18a34d028c99819146b532de7216b6e
9c631db79175e6a18d180300ffa75bafa36025721ede7efea2949512bd0a
f4f25e3ebc5d194a405dc57fe1da0599e2f8b1c21ad01a1557dd10d4a5b5
b34dbcf76046fc6f60ab5d06006f13061fab336ade7ed14a7df7a9dce32d
277bcfb6ff456931e91933b1c895aa79cfd235c39fcb83f4528475712001
7e7a44a8c2be423c71c1be7eee9d0a2b5572e39e9dd6b4af5a118172dfa2
5347d0061ed0208e30bb0119f4c66fa4642b4612b68c8c7df7cdce862ad7
efe55c615603fa3fa77f8929f99d236c927f0d2bb00f382c42030c1b7ff0
```

Activate the BIG-IP system license

If your BIG-IP system is not yet licensed to you, you may be prompted for the base registration key or an add-on registration key.

To activate the license on the BIG-IP system using the Configuration utility, you can use either the automatic activation method or the manual activation method. The activation method specifies the method by which you want the system to communicate with the F5 license server.



Note To activate the license on the BIG-IP system at the command line, see AskF5 article: [SOL2595: Activating and installing a license file at the command line.](#)



You can use the automatic method if the BIG-IP management port is configured to route traffic to the Internet. You should use the manual method if the BIG-IP management port is not configured to route traffic to the Internet.

To activate a license using the manual activation method

1. Log in to the Configuration utility.
2. Click **Activate**.
3. Click **Manual** and then click **b**.
4. Copy the dossier.
5. Navigate to the [F5 Product Licensing](https://secure.f5.com) page (secure.f5.com).
6. In the row that lists BIG-IP 9.x and later, click **Activate License**.
7. Paste the dossier into the **Enter your dossier** field, and then click **Next**.
8. Copy the license returned by the [F5 Product Licensing](https://secure.f5.com) page and paste it into the **License** field in the Configuration utility.
9. Click **Next**.



Note If this is a new BIG-IP system, when logging in, open a web browser on a work station attached to the network on which you configured the management port. Then, type the following URL in the browser: **https://<IP address>/. <IP_address>** is the address you configured for the management port.



Important Traffic processing is briefly interrupted while the BIG-IP system reloads the configuration



Activate an add-on module

BIG-IP feature modules can be added to a BIG-IP device for additional functionality. Adding a feature module requires you to obtain an add-on registration key, and re-activate the license. After you obtain an add-on registration key, you can activate the feature using the Configuration utility.

The format of the BIG-IP Add-On registration key is as follows:

AAAAAAA-BBBBBBB

To re-activate the license with the Add-On registration using the manual activation method

1. Log in to the Configuration utility.
2. Click **System**, click **License**, and then click **Re-activate**.
3. Paste the Add-On registration key into the **Add-On Key** field and click **Add**.
4. Click **Manual**, and then click **Next**.
5. Copy the dossier.
6. Go to the [F5 Product Licensing](https://secure.f5.com) page (secure.f5.com).
7. In the row that lists BIG-IP 9.x and later, click **Activate License**.
8. Paste the dossier into the **Enter your dossier** field, and then click **Next**.
9. Copy the license returned by the [F5 Product Licensing](https://secure.f5.com) page and paste it into the **License** field in the BIG-IP Configuration utility, and then click **Next**.



Important Traffic processing is briefly interrupted while the BIG-IP system reloads the configuration



Provision licensed modules in your BIG-IP system

Before you can use a module properly, it must be provisioned.

To provision a licensed module using the Configuration utility

1. Go to **System > Resource Provisioning**.
2. Select the check box for each licensed module.
3. Select either **Minimum** or **Nominal** for each licensed module.
4. After making the necessary provisioning changes, click **System**.
5. Click **Configuration**, click **Device**, and then click **Reboot** to restart the system.
6. When prompted, click **OK** to confirm the restart operation.

Validate license compliance levels

vCMP Guests

The vCMP license allows you to deploy the maximum number of guests that the specific blade platform allows. For more information, see AskF5 article: [SOL14218: vCMP guest memory/CPU core allocation matrix](#).

When the licensed compression limit has been exceeded, two indicators are provided:

- The BIG-IP system logs the following message to the `/var/log/ltm` file:

```
Compression license limit of <limit> Mbit/s exceeded today
```

- The BIG-IP system will log this message once per day.

```
bigipCompLimitExceeded ("The compression license limit is exceeded.")
```

The BIG-IP system sends an SNMP trap with the following Object ID: OID=.1.3.6.1.4.1.3375.2.4.0.35.

SSL TPS license

When SSL TPS limits have been reached, a log message will show up in `/var/log/ltm` as follows:

```
tmm tmm[1253]: 01260008:3: SSL transaction (TPS) rate limit reached
```



Tip Technicians can search for the above message to determine if they have exceeded these limits recently. In addition, reviewing performance graphs for current SSL TPS and compression levels may provide guidance on purchasing additional licenses.



Additional resources

The following table points to additional resources you can visit to learn more about the concepts and areas mentioned in this chapter. You can find AskF5 solution articles and the right product manuals for your software version by searching [AskF5 \(support.f5.com\)](https://support.f5.com).

Table 7.1: Additional resources

For more information about	See
License activation prior to software upgrades.	SOL7727: License activation may be required prior to software upgrade for the BIG-IP or Enterprise Manager system.
Finding the serial number or reg key on your system.	SOL3782: Finding the serial number or registration key of your BIG-IP system.
SSL TPS licensing limits.	SOL6475: Overview of SSL TPS licensing limits.
Determining BIG-IP compression capabilities.	SOL13469: Determining the compression capability of your BIG-IP system (11.x).
Alert actions when compression limits are reached.	SOL7313: The HTTP compression value in a license indicates the maximum rate at which compression is performed on HTTP data.
BIG-IP ASM attack signature updates.	SOL8217: Updating the BIG-IP ASM attack signatures.

Help improve this guide

Please help F5 improve this guide by responding to a few questions about this chapter.

(Note: You must be viewing this document in Adobe Acrobat Reader or similar to use this form.)

Did this chapter answer all of your questions about the subject matter? Yes No

If not, what information should be included that is not? _____

Did you find any errors pertaining to subject matter in this chapter? Yes No

If yes, please describe the error: _____

If yes, please copy and paste the paragraph containing the error here: _____

Did you find non-subject-matter errors in this chapter (spelling, etc.)? Yes No

If yes, please describe the error: _____

If yes, please copy and paste the paragraph containing the error here: _____



Backup and Data Recovery

At a glance—Recommendations

F5 has identified the following backup and data recovery recommendations:

- Create a user configuration set (UCS) archive and store the file on a remote backup server.
- Create a UCS archive before and after making significant changes to your system and before upgrades.
- Store UCS archive files on a secure remote backup server.
- Restore a UCS archive on the same unit in which the archive was created, or same platform type in the case of a return materials authorization (RMA).
- Create a single configuration file (SCF) if you are planning to copy the configuration across multiple BIG-IP systems.
- Load the default SCF to restore the factory default settings.

Background

This section provides context for our recommended procedures in the form of overviews and supplemental information. It includes the following topics:

- UCS archives.
- Backing up configuration data.
- Restoring configuration data.
- SCFs.

BIG-IP software offers two supported methods for backing up and restoring the configuration: UCS archives and SCFs. To create, delete, upload, or download an archive, you must have either the administrator or resource administrator role privileges.

UCS archives

A UCS archive contains BIG-IP configuration data that can fully restore a BIG-IP system in the event of a failure or RMA.

Each time you back up the configuration data, the BIG-IP system creates a new UCS archive file in the **/var/local/ucs** directory. In addition to configuration data, each UCS file contains various configuration files necessary for the BIG-IP system to operate correctly.

A UCS archive contains the following types of BIG-IP system configuration data:

- System-specific configuration files (traffic management elements, system and network definitions, and others).
- Product licenses.



- User accounts and password information.
- Domain Name Service (DNS).
- Zone files.
- Installed SSL keys and certificates.



Important A typical UCS archive contains the SSL private keys associated with client and server SSL profiles. It also contains user accounts, passwords, and critical system files, unless explicitly excluded during the backup process.

If your UCS archive contains SSL private keys, store backup UCS archives in a secure environment.

Back up and restore configuration data

You can use UCS archives to back up and restore the data. F5 recommends using this feature to mitigate potential loss of BIG-IP system configuration data.

Determine archiving frequency

F5 recommends creating an archive at the following times:

- On a monthly basis for backup purposes. F5 recommends storing the file on a remote backup server.
- Before you upgrade a BIG-IP system.
- Before and after you make significant changes to your system, such as adding or modifying iRules or editing configuration settings.
- According to your company practices and/or specific industry requirements.

Save UCS archives

When you save a UCS archive, by default, the system stores it in the directory **/var/local/ucs**. Archives located in a directory other than the default do not appear in the list of available archives when using the Configuration utility to create or restore a UCS archive, or when using the **list /sys ucs** command in the tmsh utility.

To identify the file easily, F5 recommends that you include the BIG-IP host name and current timestamp as part of the file name.

F5 recommends keeping a backup copy of your UCS archives on a secure remote server. In the unlikely event you need to restore your BIG-IP system and are unable to access the **/var /local/ucs** directory on your BIG-IP system, you can upload the backup file from the remote server and use it to restore your system.



Important A typical UCS archive contains the SSL private keys associated with client and server SSL profiles. It also contains user accounts, passwords, and critical system files, unless explicitly excluded during the backup process.

If your UCS archive contains SSL private keys, store backup UCS archives in a secure environment.



Note If you set **Encryption** to **Enabled** under **System > Archives > General Properties** when creating an archive, the BIG-IP system encrypts the UCS archive file.

Restore configuration data from a UCS archive

When restoring configuration data, F5 recommends that you run the same version of the BIG-IP software on the BIG-IP system from which it was backed up. However, you can restore a BIG-IP v10.x UCS archive on a system running BIG-IP v11.x software.

F5 also recommends that you only restore a UCS file to another platform of the same model as the one where the UCS file was created. Certain core hardware changes can cause a UCS to fail to load properly on dissimilar hardware, requiring manual intervention to correct.

For more information about restoring archive data, see [Restore data from a BIG-IP system UCS archive](#). If your system configuration has been customized to reference files that are not included in the default BIG-IP installation, see AskF5 article: [SOL4422: Viewing and modifying the files that are configured for inclusion in a UCS archive](#).

For more information, see AskF5 article: [SOL175: Transferring files to or from an F5 system](#).



SSL private keys with passphrases

If you are restoring on a new system, a UCS archive that includes SSL private keys with encrypted passphrases cannot be decrypted by the new system. This format is an intentional security measure.

When replacing one system of a high availability (HA) pair, F5 recommends that you configure basic networking on the replacement unit and synchronize the configuration from its peer rather than restoring it from a UCS archive. Synchronizing the units allows the peer to share the master key with the new system.

If you cannot synchronize the original master key to the new system from its peer but you know the original unencrypted passphrases, you can install the UCS file to restore the configuration, modify the affected SSL profiles to replace the encrypted passphrases with unencrypted versions, and save the resulting configuration.

If you are restoring a backup that contains SSL private key passphrases after reinstalling the operating system, replacing a failed system with a new system, or otherwise moving an existing configuration to a new system, the encrypted passphrases for SSL private keys used in the configuration cannot be decrypted. An error message similar to the following example appears:

```
BIGpipe client SSL profile creation error:
01070937:3: Master Key decrypt failure - decrypt failure
```

If you receive this error message when installing the UCS archive, before going further, see AskF5 article: [SOL9420: Installing a UCS file containing an encrypted passphrase](#).

Use UCS archive to restore a system outside the device cluster

You can install a UCS file onto a BIG-IP system that is outside the cluster of the system that generated the archive. The SecureVault key is hard-coded into the device hardware, so the SSL private key passphrases will not be decrypted.

Install UCS archive on BIG-IP DNS

If you want to install a UCS archive on a BIG-IP DNS™ (formerly Global Traffic Manager/GTM) system, for an RMA replacement for example, and prevent the BIG-IP DNS system from synchronizing the contents of the UCS archive to the BIG-IP DNS synchronization group, see AskF5 article: [SOL14083: Preventing synchronization when installing a UCS archive on a BIG-IP GTM](#)



[system.](#)

For a BIG-IP DNS RMA unit that is licensed and provisioned with the BIG-IP DNS module and the DNSSEC feature, see AskF5 article: [SOL13542: Restoring DNSSEC configuration data to a BIG- IP GTM RMA unit.](#)

Restore a UCS file with BIG-IP Application Security Manager

If you are restoring a UCS file that is licensed and provisioned with the BIG-IP ASM module, you may need to provision the system for BIG-IP ASM before loading the UCS file. For more information, see AskF5 article: [SOL13945: The BIG-IP ASM MySQL database is not installed completely if BIG-IP ASM is not provisioned when the UCS is loaded.](#)

Restore a UCS file on a redundant pair

If you are restoring a UCS file on a BIG-IP unit that is part of a redundant pair, see [AskF5 article: SOL8086: Replacing a BIG-IP system in a redundant pair without interrupting service.](#)

Restore a UCS file on a vCMP host or vCMP guest

For a Virtual Clustered Multiprocessing (vCMP) host, the UCS configuration archive contains only the necessary files that are required to restore the vCMP host configuration, but does not include the vCMP guest virtual disk.

For a vCMP guest, the UCS configuration archive contains all of the files that are specific to the vCMP guest, including the configuration files, local user accounts, and SSL certificate and key pairs.

When you restore a vCMP host UCS archive on an appropriate vCMP host, the vCMP host automatically attempts to restore the vCMP guest to a base state by doing the vCMP guest provisioning, installation, and deployment. When the vCMP guest has been restored to a base state, you can restore the vCMP guest by installing the UCS archive that was previously taken from a vCMP guest. The restoration of a UCS archive to a vCMP guest is subject to all of the restrictions and considerations described in the previous sections of this article

Exceptions to UCS archive file on VIPRION systems

The BIG-IP VIPRION system is unique among BIG-IP hardware in that it allows you to combine all blades within the chassis to increase processing ability. This functionality, referred to as clustering, is unique and is written to a special file in the **/shared/db** directory called **cluster.conf**.

Additionally, the system saves a copy as **cluster.conf.<chassis SN>**, where **<chassis SN>** is the unique serial number of the chassis. The blade maintains the ***.<chassis SN>** files and copies them to **cluster.conf** when the blade starts in a chassis that it has encountered before.

The **cluster.conf** file consists of each blade's copy of the cluster configuration. It contains the management addresses for the cluster and for each blade within the cluster, as well as other cluster-specific information. Since this information is specific and unique to the chassis, the information is not included within a UCS archive.

If you load a UCS archive, the archive does not overwrite the current cluster.conf file and does not restore a previous cluster_



configuration. If you reconfigure the cluster, you must manually rebuild the **cluster.conf** file in the following circumstances:

- A blade starts as the primary blade in the chassis, and the **cluster.conf** file does not contain the serial number of the chassis.
- You have replaced the chassis. (The chassis serial number must match the chassis serial number in the **cluster.conf** file.)

For more details on replacing a VIPRION chassis, see AskF5 article: [SQL14302: Replacing a VIPRION chassis that has one or more blades installed](#).

Licensing

The BIG-IP license is associated with a specific hardware serial number. The UCS archive contains the license of the BIG-IP system from which the configuration was saved.

To install a UCS archive file on a BIG-IP system successfully, you must do one of the following actions:

- Restore the UCS archive to the same system from which it was saved.
- Relicense the BIG-IP system after restoring the UCS archive.
- Save the license file prior to restoring the configuration from another system, and then copy the license file back.
- Install the UCS archive by using the tmsh no-license option.
- Contact F5 Technical Support to have the license associated with the serial number of a new system.



Important F5 Technical Support will associate a license file with a new serial number only on an as-needed basis in the event of a return materials authorization (RMA).

If you use a different license than the one contained in a restored UCS archive, the replacement license must include authorization for the same options and add-on modules, such as BIG-IP WebAccelerator™ or BIG-IP ASM.

If you attempt to restore a UCS configuration referencing an unlicensed module, the BIG-IP system does not properly restore the UCS archive.

Additionally, the BIG-IP system reports a Provisioning Warning message in the Configuration utility, as well as the status of **ModuleNotLicensed** in its command-line prompt.



SCFs

A single configuration file (SCF) is a flat, text file that contains a series of bigpipe commands, and the attributes and values of those commands, that reflect the configuration of the BIG-IP system. Specifically, the SCF contains the local traffic management and TMOS configuration of the BIG-IP system.



Note An SCF does not contain SSL certificate or key files.

F5 recommends creating an SCF when you are planning to migrate the BIG-IP configuration to another device.

You can use an SCF to copy system configuration to multiple BIG-IP systems. This will help create a secure and consistent LTM environment on your network.

For added security, F5 recommends the SCF to a remote location until you are ready to install.

For more information, see Ask F5 article: [SOL13408: Overview of single configuration files \(11.x\)](#).

File location and naming

By default, SCF files are saved to the **/var/local/scf/** directory with the name you specify and the **.scf** extension. Example:

```
tmsh save /sys config file bigip1
```

The previous command saves the current configuration as **/var/local/scf/bigip1.scf**.

Install an SCF

When you install an SCF on a target BIG-IP system, the system first saves the currently running configuration to the **/var/local/scf/backup.scf**, and then loads the specified SCF into running memory. For example, the **tmsh load /sys config file bigip1** command saves the currently running configuration to the **/var/local/scf/backup.scf** before loading the **/var/local/scf/bigip1.scf** on the system.



Note Run **tmsh save sys config** to save the current BIG-IP system configuration to an SCF. Unsaved changes will not be reflected in the SCF.

Use an SCF to restore a BIG-IP system configuration to factory default settings

You can load the default SCF to reset the BIG-IP configuration to the factory default setting. When you restore the BIG-IP configuration to factory default settings, the system does the following tasks:

- Removes all BIG-IP local traffic configuration objects.
- Removes all BIG-IP network configuration objects Removes all non-system maintenance user accounts.



- Retains the management IP address.
- Removes system maintenance user account passwords (root and admin).

Procedures

Follow the procedures detailed in this section to guide you in managing backups and ensuring data recovery runs smoothly:

Use the `tmsh help sys config` command

For information regarding the options available you can use the `tmsh help sys config` command. This procedure is an example that shows how to get information regarding the user-only option.

To use `tmsh help sys config` at the command line

1. Log in to the Traffic Management Shell (tmsh) by typing the following command:

```
tmsh
```

2. At the command prompt, type:

```
help /sys config
```

3. At the command prompt, type:

```
user-only
```

4. Press **Enter**.
5. To move to the next instances of the user-only option, press **n**.
6. To exit from the tmsh command help, press **q**.
7. To exit tmsh, type quit, then press **Enter**.



Tip You can also navigate through the tmsh help using the Up and Down arrows on your keyboard.



View a list of existing UCS archives

You can view a list of archives (UCS files) that are currently stored in the **/var/local/ucs** directory on the BIG-IP system. When you view a list of archives, the Configuration utility displays the following information:

- The name of the UCS file.
- The date that the UCS file was created or uploaded.
- The size of the file.

To view a list of existing archives using the Configuration utility

- Go to **System > Archives**.

A list of existing UCS files displays.



Note If you have upgraded your BIG-IP system, a UCS file named **config.ucs** was created in the process. This UCS file should appear in this list.

Create and save a UCS archive on the BIG-IP system

When you create a new archive, unless otherwise directed, the BIG-IP system automatically stores it in a default location, the **/var/local/ucs** directory. You can create as many archives as you want, as long as each archive has a unique file name.

You can specify that the BIG-IP system store an archive in a directory other than **/var/local/ucs**; however those archives will not display in the Configuration utility **Archives** list.

All boot locations on a BIG-IP system use the same **/shared** directory, which makes it a good choice for a UCS save location. Saving an archive to the **/shared** directory will allow you boot to another boot location and access the archive. This can greatly simplify recovery from a variety of issues.

When you create an archive, you can configure some settings. The following table lists and describes these settings. If default values exist, those are also shown.


Table 8.1 Default UCS archive encryption values

Settings	Description	Default value
File Name	Specifies the file name for the archive. You do not need to specify the UCS file name extension. The BIG-IP system appends the UCS extension automatically.	No default value
Encryption	Enables or disables encryption of the archive. If you select Enabled, you will be asked to type and verify a Passphrase	Disabled
Passphrase	Specifies a password that a user must use to decrypt an archive.	No default value
Verify Passphrase	Specifies the password that you defined with the Passphrase setting.	No default value
Private Keys	Specifies whether to include or exclude private keys in the archive.	Included
Version	Displays the version of the BIG-IP system application that is currently running on the BIG-IP hardware platform. You cannot configure the Version field.	No default value

**To create a UCS archive file using the Configuration utility**

1. Go to **System > Archives**.
2. Click **Create**.



Note If the **Create** button is unavailable, you do not have permission to create an archive. You must have administrator role privileges assigned to your user account to create an archive.

3. Type a unique file name.

F5 recommends that the file name match the name of the BIG-IP system. For example, if the name of the BIG-IP system is **bigip2**, then the name of the archive file should be **bigip2.ucs**.



Important You must use a unique file name. If a file by the same name already exists, the UCS archive file is not created and the system displays a warning message that appears similar to the following example:

The file already exists on the system

4. If you want to encrypt the archive, for **Encryption** select **Enabled**.
5. If you want the BIG-IP system to include any private keys, select **Include for Private Keys**. If you choose to include private keys, be sure to store the archive file in a secure environment.
6. Click **Finished**.
7. Once the data has been backed up and the file created, click **OK**.

To download and copy an archive to another system using the Configuration utility

1. Go to **System > Archives**.
2. Click on the UCS file name you want to download.
3. In the **General Properties** field, click **Download <filename.ucs>**.
4. Select **Save file** and save the file.
5. Find the file in your computer's Downloads folder and copy it.



To create a UCS archive file using tmsh at the command line

1. Log in to Traffic Management Shell (tmsh) by typing the following command:

```
tmsh
```

2. Save your running configuration by typing the following command:

```
save sys config
```

3. Create the UCS archive file by typing the following command syntax:

```
save /sys UCS </path/to/ucs>
```

Replace **<path/to/ucs>** with the full path to the UCS archive file.

For example:

```
save /sys UCS /var/tmp/Myucs.ucs
```

Optional: If you want to encrypt the UCS archive with a passphrase, type the following command syntax:

```
save /sys UCS <path/to/ucs> passphrase <password>
```

Replace **<path/to/ucs>** with the full path to the UCS archive file, and replace **<password>** with the passphrase you want to use to encrypt the UCS archive. For example:

```
save /sys UCS /var/tmp/Myucs.ucs passphrase password
```

Optional: If you want to exclude SSL private keys from the UCS archive, type the following command syntax:

```
save /sys ucs <path/to/ucs> no-private-key
```

Replace **<path/to/ucs>** with the full path to the UCS archive file. For example:

```
save /sys ucs /var/tmp/Myucs.ucs no-private-key
```

4. Copy the UCS file to another system.

View UCS archive properties

Using the Configuration utility, you can view the properties previously created archives.



Note You cannot modify the properties of an archive. If you want to make changes, you have to delete the archive and create a new one.



The viewable properties of an archive include:

- The name of the archive.
- The version of the BIG-IP system on which the archive was created.
- The encryption state of the archive (encrypted or unencrypted).
- The date that the archive was created.
- The size of the archive.

To view the properties of an archive using the Configuration utility

1. Go to **System >Archives**.
2. Click the name of the archive that you want to view.

The archive's **General Properties** display.

Restore data from a BIG-IP system UCS archive

In the unlikely event that the BIG-IP system configuration data becomes corrupted, you can restore the data from the archive that is currently stored in the directory **/var/local/ucs**. If no archive exists in that directory, then you cannot restore configuration data.



Note The BIG-IP system replaces any existing configuration with the UCS archive file configuration.



To restore a configuration in a UCS archive using the Configuration utility

1. Go to **System > Archives**.
2. Click the name of the UCS archive you want to restore.

If the UCS archive is encrypted, type the passphrase for the encrypted UCS archive file in the **Restore Passphrase** field.

3. To initiate the UCS archive restore process, click **Restore**.

When the restore process is completed, examine the status page for any reported errors before proceeding to the next step.

4. To return to the **Archive List** page, click **OK**.

If you restore a UCS archive on a different device and receive activation errors, you will need to reactivate the BIG-IP system license. To ensure that the configuration is fully loaded after relicensing, restart the system by navigating to **System > Configuration**, then click **Reboot**.

If the system you restored contains the FIPS 140 HSM, you must configure the FIPS 140 HSM Security World.

For additional information about recovering FIPS information after a system recovery, see [Configuring and Maintaining a FIPS Security Domain](#) chapter in [Platform Guide: 6900](#) or [Platform Guide: 8900](#).

To restore configuration data using tmsh at the command line

1. Log in to Traffic Management Shell (tmsh) by typing the following command:

```
tmsh
```

2. Restore the UCS archive file by using the following command syntax:

```
Replace <path/to/ucs>
```

Use the full path of the UCS archive file you want to restore using the following command syntax:

```
load /sys UCS <path/to/ucs>
```



Note If you do not specify the path, the BIG-IP system will look for the UCS archive file in the default **/var/local/ucs** directory.



If the UCS archive file was encrypted during backup, you will be prompted to type the passphrase for the archive file.

Optional: If you are running your BIG-IP system on 6400, 6800, 8400, or 8800 hardware platform, type the following command to switch to the bash shell:

```
run /util bash
```

To verify that the new or replaced secure shell (SSH) keys from the UCS file are synchronized between the BIG-IP system and the Switch Card Control Processor (SCCP) type the following command:

```
keyswap.sh sccp
```

3. At the command prompt, type to switch back to tmsh:

```
exit
```

4. Restart the system by typing the following command:

```
reboot
```

If you installed the UCS archive on the same device on which the backup was created, it will load the restored configuration after the system restarts. If you restored the backup on a different device and received a reactivation error, you must reactivate the BIG-IP system license. Alternatively, you can replace the **/config/bigip.license** file with the original bigip.license file that you backed up from the target system.

If the system you restored contains the FIPS 140 HSM, you must configure the FIPS 140 HSM Security World. For additional information about recovering FIPS information after a system recovery, see [Configuring and Maintaining a FIPS Security Domain chapter](#) in [Platform Guide: 6900](#) or [Platform Guide: 8900](#).

Restore a UCS on a replacement RMA unit

F5 recommends that you use the following procedure when you restore the archive on a different device than the system on which the backup was created, such as an RMA system. If you do not use this procedure when restoring the archive on a different device, the configuration load may fail and the mcpd process generates an error message that appears similar to the following example to both **stdout** and the **/var/log/ltm file:mcpd[2395]**:

```
01070608:0: License is not operational (expired or digital signature does
not match contents).
```

F5 expects this message, and you can correct the issue by re-licensing the system, which is discussed later in the procedure.

To restore configuration data on a replacement RMA unit using tmsh at the command line

1. Activate the license on the unit according to the steps detailed AskF5 article: [SOL7752: Overview of licensing the BIG-IP system](#).
2. Log in to the Traffic Management Shell (tmsh) by typing the following command:



```
tmsh
```

3. Restore the UCS archive file by using the following command syntax.

```
load /sys UCS <path/to/ucs> no-license
```

4. Replace **<path/to/ucs>** with the full path of the UCS archive file you want to restore.
5. If the UCS archive file was encrypted with a passphrase during the backup, you are prompted to type the passphrase for the archive file.
6. If you are running the BIG-IP system on a 6400, 6800, 8400, or 8800 hardware platform, switch to the bash utility by typing the following command:

```
run /util bash
```

7. To verify that the new or replaced SSH keys from the UCS file are synchronized between the BIG-IP and the SCCP, type the following command:

```
keyswap.sh sccp
```

8. To switch back to tmsh, type the following command:

```
exit
```

9. Restart the system by typing the following command:

```
reboot
```



Note If you do not specify the path, the BIG-IP system does as if the UCS archive file is located in the default **/var/local/ucs** directory.

If the system you restored contains the FIPS 140 HSM, you must configure the FIPS 140 HSM Security World after completing steps 1 through 5. For additional information about recovering FIPS information after a system recovery, see [Configuring and Maintaining a FIPS Security Domain](#) in Platform Guide: 6900 and 8900.

Restore UCS archives on BIG-IP systems running newer software versions

F5 recommends that you restore a UCS archive on a system running the same BIG-IP software version as the system you used to create it. It is possible to restore a UCS archive on a system running a newer software version, if the older version is supported by the upgrade.

For example: there is a supported upgrade path between BIG-IP v10.x and BIG-IP v11.x, so you can successfully restore a BIG-IP v10.x UCS archive file on a BIG-IP system running v11.x. However, there is no supported upgrade path between BIG-IP v9.x and BIG-IP v11.x, so you cannot restore a BIG-IP v9.x UCS archive file on a BIG-IP system running v11.x.

For information about supported upgrade paths, see the product release notes for your specific software version.



To restore UCS archives on BIG-IP systems running newer software versions

1. Verify that a supported upgrade path exists between the software version from which the UCS archive was obtained and the software version running on the target system.
2. Manually copy the UCS archive file to the **/var/local/ucs/** directory on the target system.
3. Restore the UCS archive on the BIG-IP system.

If you are restoring the archive on a different device than the system on which the backup was created, follow the [Restore a UCS on a replacement RMA unit](#).



Important The BIG-IP system replaces any existing configuration with the UCS archive file configuration.

Download a UCS archive to a remote system

You can download a copy of an existing archive to a remote system. This feature protects the configuration data in the unlikely event you need to restore your BIG-IP system and are unable to access the **/var /loca/ucs** directory on your BIG-IP system.

When you download an existing archive, you first display the properties of the archive you want to download, and then specify the complete path name of the location where you want to save the archive copy.

To download an archive using the Configuration utility

1. Go to **System > Archives**.
2. Click the name of the archive that you want to view.

The General Properties for that archive display.

3. Click **Download: <ucs filename>**.
4. Click **Save**.

The BIG-IP system downloads a copy of the UCS file to the system from which you initiated the download.

Upload a UCS archive from a remote system

If a UCS archive on your BIG-IP system is unavailable or corrupted for some reason, you can upload a previously created archive copy from a remote or backup system to replace it.



To upload an archive using the Configuration utility

1. Go to **System > Archives**.
2. Click **Upload**.
3. Type the complete path and file name of the archive that you want to upload onto the BIG-IP system.

If you do not know the path or file name, click **Browse** and go to the location.

4. For the **Options** setting, select the **Overwrite existing archive file** field if you want the BIG-IP system to overwrite any existing archive file.
5. Click **Upload**.

The specified archive uploads to the **/var/local/ucs** directory on the BIG-IP system.



Note The BIG-IP system overwrites an existing file with the uploaded file only when the name of the archive you are uploading exactly matches the name of an archive on the BIG-IP system.

Delete a UCS archive

You can use the Configuration utility to delete any archive on the BIG-IP system that is stored in the directory **/var/local/ucs**.

To delete an archive using the Configuration utility

1. Go to **System > Archives**.
2. Select the check box next to the name of the file you want to delete.
3. Click **Delete**.
4. Click **Delete** again.

The archive is deleted from the **/var/local/ucs** directory on the BIG-IP system.

Manage UCS files for a VIPRION

When managing UCS archives for the VIPRION platform, F5 recommends that you create the UCS archive while connected to the mgmt port. Doing so ensures that the UCS contains configuration data from all VIPRION blades in the chassis.

Restore a UCS archive to a different hardware platform

Restoring a UCS archive to a hardware platform other than the one used to create the archive is not supported. F5 recommends using an SCF instead.



Work with SCFs

To view a list of the existing SCFs on the BIG-IP system using tmsh at the command line

1. Log in to the Traffic Management Shell (tmsh) by typing the following command:

```
tmsh
```

2. To display the list of SFC files, type the following command:

```
list /sys config file.
```

To create and save an SCF on the BIG-IP system using tmsh at the command line

3. Log in to the Traffic Management Shell (tmsh) by typing the following command:

```
tmsh
```

4. To save the running configuration to an SCF, type the following command syntax:

```
save /sys config file <name>
```

The SCF is saved to the **/var/local/scf/** directory.



Important Store the backup SCFs containing sensitive information in a secure location.

**To view the properties and contents of the SCF at the command line**

- Type a Linux command such as **cat** to view the contents of the SCF.

Example:

```
cat the /var/local/scf/scf_filename
```

To restore data from an SCF using tmsh at the command line

1. Log in to the Traffic Management Shell (tmsh) by typing the following command:

```
tmsh
```

2. To install an SCF on a BIG-IP system, type the following command syntax:

```
load /sys config file <name>
```

3. Type **Y** at the following prompt to load the SCF:

```
Replace the running configuration? (y/n)
```

To copy configuration data to a different platform using SCF

1. Build a BIG-IP LTM template configuration by configuring a system using the Configuration utility or tmsh.
2. Save an SCF from the fully-configured system using the **tmsh save /sys** command.
3. Store the SCF in a secure location.

The SCF can be used as a template to configure future BIG-IP systems.

4. When you are ready to use the SCF to configure a new BIG-IP system, copy the SCF to the new BIG-IP system, then edit the SCF using a text editor prior to importing it.

For example: Change the IP addresses, routing information, interface settings and other common settings, as needed.



Note SCFs are version-specific. In versions 11.5.0 and later, there are version-specific parsers for all supported versions. For previous versions, you may need to take note of both syntax and semantic differences when migrating between versions.

5. To install the SCF into a new system using the **tmsh load /sys** command.

To delete an SCF using tmsh at the command line

1. Log in to the Traffic Management Shell (tmsh) by typing the following command:

```
tmsh
```

2. To delete the SCF, use the following syntax:



```
delete /sys config file <file _ name>
```

For example, to delete the SCF named 'bigip1', type the following command:

```
delete /sys config file bigip1
```

Use the SCF to restore the factory default settings

To restore the BIG-IP configuration to the factory default setting using tmsh at the command line

1. Log in to the Traffic Management Shell (tmsh) by typing the following command:

```
tmsh
```

2. At the command prompt, type:

```
load sys config default
```

3. Type **Y** at the following prompt:

```
Reset the system configuration to factory defaults? (y/n)
```

4. Save the change by typing the following command:

```
save sys config partitions all
```



Note When managing SCFs for the VIPRION platform F5 recommends that you create the SCF while connected to the mgmt port.



Additional resources

The following table points to additional resources you can visit to learn more about the concepts and areas mentioned in this chapter. You can find AskF5 solution articles and the right product manuals for your software version by searching [AskF5](#) (support.f5.com).

Table 8.2: Additional resources

For more information about	See
UCS archives.	SOL4423: Overview of UCS archives.
Backing up and restoring UCS files.	SOL13132: Backing up and restoring BIG-IP configuration files (11.x).
Working with encrypted UCS files.	SOL8465: Viewing and extracting the contents of an encrypted UCS archive file.
Working with files configured for inclusion in a UCS file.	SOL4422: Viewing and modifying the files that are configured for inclusion in a UCS archive.
Working with SCFs.	SOL13408: Overview of single configuration files (11.x).

Help improve this guide

Please help F5 improve this guide by responding to a few questions about this chapter.

(Note: You must be viewing this document in Adobe Acrobat Reader or similar to use this form.)

Did this chapter answer all of your questions about the subject matter? Yes No

If not, what information should be included that is not? _____

Did you find any errors pertaining to subject matter in this chapter? Yes No

If yes, please describe the error: _____

If yes, please copy and paste the paragraph containing the error here: _____

Did you find non-subject-matter errors in this chapter (spelling, etc.)? Yes No

If yes, please describe the error: _____

If yes, please copy and paste the paragraph containing the error here: _____



Software Updates

At a glance—Recommendations

F5 has identified the following software update recommendations:

- Subscribe to F5 TechNews and Security mailing lists.
- Check for software updates.
- Find the latest software.
- Check for OPSWAT downloads.
- Download and install updates to the IP geolocation database.
- Check for BIG-IP ASM and DPI signatures.

Background

This section provides context for our recommended procedures in the form of overviews and supplemental information.

In versions 11.5.0 and later, F5 the **Automatic Update Check** (phone home) feature is enabled by default.

If your device has access to the F5 software download servers using the internet, this feature automatically checks for BIG-IP software updates on a weekly basis and lists the updates in the Configuration utility, including relevant links.

If you use this feature, you will not have to check for the latest software updates manually. For more information see AskF5 article: [SOL15000 Using the Automatic Update Check feature](#).

In addition to updates to the BIG-IP operating software, F5 provides additional updates for features like the IP Geolocation database, OPSWAT, and BIG-IP ASM security updates. Updates for these features are managed separately from the core BIG-IP updates. F5 recommends that administrators keep these features updated to ensure your BIG-IP system has current information and protection against the latest security threats.



Note You can only do major software upgrades if the BIG-IP system is entitled under a current technical support contract. For more information about entitlement, see [Licenses and Entitlement](#).



Procedures

Follow the procedures detailed in this section to guide you in updating your BIG-IP system software.

Get security updates

F5 recommends regular and timely acquisition of F5 security updates, BIG-IP ASM attack signature updates, and OPSWAT updates.

When F5 discovers remote vulnerabilities, F5 implements, tests, and releases security hotfixes for any vulnerable, supported version and sends an email alert to the F5 Security mailing list. F5 encourages customers with an active support account to subscribe to this list. For more information, see AskF5 article: [SOL4602: Overview of the F5 security vulnerability response policy](#).

To sign up for security mail lists

1. Go to [AskF5 \(support.f5.com\)](#).
2. From the **Self-Help** menu, click **Subscribe: Mailing Lists**.
3. Type your email address.
4. Select **Security Updates**, and click **Submit**.

Subscribe to TechNews

AskF5 offers two TechNews email publication options:

- TechNews Weekly HTML eNewsletter includes timely information about known issues, product releases, hotfix releases, updated and new solutions, and new feature notices.
- TechNews Notifications is a plain-text email that is sent any time a product or hotfix is released. This information is also included in the next weekly HTML TechNews email.

To sign up for the TechNews mailing lists

1. Go to [AskF5 \(support.f5.com\)](#).
2. From the **Self-Help** menu, click **Subscribe: Mailing Lists**.
3. Provide your email address.
4. Select your preferred TechNews option, and click **Submit**.

Subscribe to RSS feeds

Information about recent additions and updates to F5 products are published over RSS. You can subscribe to feeds that pertain



to specific products, product versions, and/or document sets. You can also aggregate multiple feeds into your RSS Reader to display one unified list of all selected documents.

AskF5 Recent Additions and Updates, available from the [Subscribe to RSS](#) page, provides access to all recent solutions guides, release notes, manuals, and other publications.

To generate an RSS feed

1. Go to [AskF5 \(support.f5.com\)](#).
2. From the **Self-Help** menu, click **Subscribe: RSS**.
3. Select Product, Version, Document type and Update type from the menu and click **Generate Feed**.

You will be subscribed to the RSS feed meeting your specifications.

For more information, see AskF5 article [SOL9957: Creating a custom RSS feed to view new and updated documents](#).

Find the latest software

Release notes for the version of software you want to install will contain instructions for the specific installation.

To find the latest software version for your F5 product

1. Go to the [F5 Downloads](#) page ([downloads.f5.com](#)).
2. Click **Find a Download**.
3. Find the product you want to download and click the link for the appropriate version.
4. Find and click the link for the update you want to download.
5. Read and accept the End User Software license agreement.
6. Click the file name, choose a download location, and then save the file to your computer.

Before you upgrade your BIG-IP software

Before you upgrade the BIG-IP software, review the release notes on AskF5 ([support.f5.com](#)) in the Documentation section for your product and version. Pay close attention to the following items:

- Ensure that the new version supports your hardware.
- Review the “Known issues” list.
- Review the “Behavior change” section(s).
- Review the “Upgrading from earlier versions” section.



- Review the “Upgrading from earlier configurations” section.
- Review the installation checklist.

Update OPSWAT packages for BIG-IP Access Policy Manager

The BIG-IP Access Policy Manager® (APM®) antivirus and firewall client-side checks use software libraries from a software development kit (SDK) created by OPSWAT, Inc. OPSWAT periodically issues new versions of the SDK libraries to support new security products and resolve bugs in the software. F5 distributes these updates in the form of hotfixes.

To view OPSWAT version information using the Configuration utility (BIG-IP versions 11.2.1 and later)

1. Go to **System > Software Management**.
2. Click **Antivirus Check Updates** and choose from the packages available on this device.
3. Click **Device Status**.
4. From local device / device group, select the local device or a device group you want to check.

The installed version will display.

For example:

+-----+ -----+				
Name	Status	Installed Version	Installed OESIS	Last Installed version
+-----+ -----+				
/common/bigip1121		1.0.0-192.0	3.6.5595.2	1.0.0-192.0
3.6.5595.2	success			
.test.lab				
+-----+ -----+				

To view OPSWAT version information using the Configuration utility (BIG-IP versions 11.0 - 11.2.0)

1. Go to **System > Software Management**.
2. Click **Antivirus Check Updates**.

The Installed Image area displays the F5 version, OPSWAT OESIS version, and the file date.



For example:

```
Version 1.0.0-96.0
OESIS Version 3.4.26.1
Date Thu Aug 25 08:46:44 PDT 2011
```

To view OPSWAT version information using tmsh at the command line

1. Log in to the Traffic Management Shell (tmsh) by typing the following command:

```
tmsh
```

2. Display the version by typing the following command:

```
show apm epsec software-status
```

Output will appear similar to the following example:

```
+-----+
+-----+
| Epsec::Software Device      OESIS      Previous      Previous
Status           Version  OESIS      Version      Installed
                  Version  Version      version      OESIS
Installed Version
+-----+
+-----+
| /common/          1.0.0-192.0  3.6.5595.2  1.0.0-192.0  3.6.5595.2
| success
| bigip1121.test.lab
|
+-----+
+-----+
```

To view OPSWAT version information at the command line

1. At the command prompt, type:

```
epsec version
```

2. Output will appear similar to the following example:

```
Version: 1.0.0-160.
OSDK Version: 3.5.2461.2
Installation Date: Thu Dec 6 16:25:57 PST 2014
#APM Endpoint Inspection Plugin for Linux
#APM Endpoint Inspection Plugin for Mac OS X
#APM Endpoint Inspection Libraries for Windows
```



To view OPSWAT versions available at the command line

- At the command prompt, type:

```
epsec version
```

Output will appear similar to the following example:

```
Version: 1.0.0-160.
```

```
OSDK Version: 3.5.2461.2
```

```
Installation Date: Thu Dec 6 16:25:57 PST 2012
```

```
#APM Endpoint Inspection Plugin for Linux
```

```
#APM Endpoint Inspection Plugin for Mac OS X
```

```
#APM Endpoint Inspection Libraries for Windows
```

To view available OPSWAT versions at the command line

- At the command prompt, type:

```
epsec list
```

Output will appear similar to the following example:

```
No updated endpoint security packages available.
```

```
Package: epsec-1.0.0-283.0.iso(installed)
```

```
Version:1.0.0-283.0
```

```
SDK Version:3.6.8392.2
```

To install an OPSWAT hotfix from the Configuration utility (BIG-IP APM 11.2.1 and later)

- Download the OPSWAT hotfix from the [F5 Downloads](https://downloads.f5.com) page (downloads.f5.com).



Note For instructions about how to obtain a hotfix, see AskF5 article: [SQL167: Downloading software from F5](#).

- Log in to the BIG-IP Configuration utility.
- Go to **System > Software Management**.
- Click **Antivirus Check Updates**.
- Click **Upload Package**.
- Click **Browse**.
- Select the hotfix file you downloaded.



8. On the **Install Option** menu, click the appropriate installation option.



Note The Do Not Install option uploads the EPSEC package without installing it.

9. If you selected the **Install on Autosync enabled Device Group** option, on the **Device Group** menu, click the device group.
10. Click **Upload**.
11. After the software uploads, click **OK**.



Note The upload process may take a couple of minutes.

BIG-IP APM is now running the OPSWAT package.

12. To confirm that the installation was successful, review the **Installed Version** field under the **Device EPSEC Status** tab.

To install an OPSWAT hotfix using tmsh at the command line (BIG-IP APM 11.0 and later)

1. Download the OPSWAT hotfix from the [F5 Downloads](https://downloads.f5.com) page (downloads.f5.com).



Note For instructions about obtaining a hotfix, see AskF5 article: [SQL167: Downloading software and firmware from F5](#).

2. Use a secure copy (SCP) utility to copy the file you downloaded in step 1 to the BIG-IP system's **/shared/**



apm/images folder.

3. Log in to the Traffic Management Shell (tmsh) by typing the following command:

```
tmsh
```

4. Create a new package by typing the following command:

```
create apm epsec epsec-package <package name> local-path <path/filename>
```

Replace the **<package name>** variable with the name the BIG-IP system will use to identify the package and **<path/filename>** with the path and name of the EPSEC file copied to the BIG-IP device.

Example:

```
create apm epsec epsec-package epsec-1.0.0- 196.0.iso local-path /shared/
apm/images/epsec- 1.0.0-196.0.iso
```



Note When using the Configuration utility, the BIG-IP system uses the file name as the package name by default. You may rename the package.

5. Install the new package by using the following command syntax:

```
install apm epsec epsec-package <package name>
```

Replace the **<package name>** with the name of the package you created in the previous step.

Example:

```
install apm epsec epsec-package epsec-1.0.0- 196.0.iso
```

6. To validate the package was installed, type the following command:

```
show apm epsec software-status
```

Download and install updates to the IP geolocation database

The BIG-IP system uses an IP geolocation database to source data about the origin of a name resolution request. The default database provides geolocation data for IPv4 addresses at the continent, country, state, ISP, and organization levels. The state-level data is worldwide, and thus includes designations in other countries that correspond to the U.S. state-level in the geolocation hierarchy, for example, provinces in Canada.



Note You can only access the ISP and organization-level geolocation data for IPv4 addresses using the iRules **where is** command. For more information, about iRules, search DevCentral™.



The default database also provides geolocation data for IPv6 addresses at the continent and country levels.



Tip If you require geolocation data at the city-level, contact your F5 sales representative to purchase additional database files.

You can download a monthly update to the IP geolocation database from F5.

To download and install an update to the IP geolocation database

1. Access the [F5 Downloads](https://downloads.f5.com) page (downloads.f5.com).
2. Click **Find a Download**.
3. Under **Product Line**, click the appropriate BIG-IP software branch (for example, BIG-IP v11.x).
4. Select your BIG-IP version.
5. Click **GeoLocationUpdates**.
6. Read and accept the license agreement.
7. Click the **ip-geolocation zip** file.
8. Select a download location.
9. Save the file to your computer.

To install the geolocation database update at the command line

1. Copy the ip-geolocation zip and MD5 files you downloaded from the [F5 Downloads](https://downloads.f5.com) site (downloads.f5.com) to the **/shared/tmp** directory on the BIG-IP system.
2. Log in to the command line.
3. Change the working directory to the **/shared/tmp** directory by typing the following command:

```
cd /shared/tmp
```

4. Open and extract the RPM files by typing the following command syntax:

```
unzip </path/to/zipfile>
```

Replace **</path/to/zipfile>** with the path to the zip file on the BIG-IP system:

Example:



```
unzip /shared/tmp/ip-geolocation-1.0.1- 20140627.30.0.zip
```

The output will appear similar to the following example:

```
Archive: ip-geolocation-1.0.1-20140627.30.0.zip
inflating: geoip-data-Region2-1.01.- 20140627.30.0.i686.rpm
inflating: geoip-data-ISP-2.0.1-20140627.30.0.i686.rpm
inflating: geoip-data-Org-1.0.1-20140627.30.0.i686 rpm
```

5. For each RPM file you extracted, type the following command syntax:

```
geoip_update_data -f </path/to/rpm>
```

Replace **</path/to/rpm>** with the path to the RPM file.

Example:

```
# geoip_update_data -f /shared/tmp/geoip-data-
Org-1.0.1-20120627.30.0.i686.rpm
```

The BIG-IP system installs and loads the specified database file.

6. Verify that the geolocation database was loaded with a `geoip_lookup` command to query the database. For example, the following command syntax queries one of the database files for a specific IP address:

```
geoip_lookup -f <path/to/db/files> IP
```

For example:

```
# geoip_lookup -f /shared/GeoIP/F5GeoIPOrg.dat 65.61.115.197
```

The output will appear similar to the following example:

```
opening database in /shared/GeoIP/F5GeoIPOrg.dat
size of geoip database = 180356873, version = GEO-146 20120627
Build 1 Copyright (c) F5 Networks Inc All Rights Reserved
geoip_seek = 014f0ad1
geoip record ip = 65.61.115.197 name = f5 networks
```

For information about transferring files to the F5 system, see AskF5 article: [SOL175: Transferring files to or from an F5 system](#).

Fix issues with incorrect IP geolocation installations

If you install the IP geolocation database files incorrectly, the incorrect installation might change the SELinux security context for the database files.

The BIG-IP system uses an IP geolocation database to determine the origin of an IP address. F5 releases the updates to the database in the GeoLocationUpdates container on the [F5 Downloads](#) site (downloads.f5.com). When installing or updating the IP geolocation database files, you should upload the IP geolocation ZIP archive file to the **/shared/tmp** directory on the BIG-IP



system.

When you extract the database files, the BIG-IP access control mechanism (SELinux) applies the appropriate security context to the database files, and the system installs the files to the **/shared/GeoIP** directory.

If you upload the IP geolocation ZIP archive file to a different directory on the BIG-IP system (for example, **/root/**) and then extract the database files, the SELinux module may apply the incorrect security context to the files. When this occurs, the system may fail to load the IP geolocation database properly.

Restore the proper security context to the IP geolocation database files

To restore property security context to the IP geolocation database files, you will need compare the inode numbers to verify that the TMM and gtmd processes have loaded the correct database files.

To compare inode numbers at the command line

- At the command prompt, type:

```
ls -li /shared/GeoIP/F5GeoIPISP.dat ; lsof 2>/dev/null | grep F5GeoIP
```

If the gtmd (1376259) and TMM (80575) inode numbers do not match for the F5GeoIPISP.dat database file, the output will appear similar to the following example:

```
1376259 /shared/GeoIP/F5GeoIPISP.dat
gtmd 5871 root mem REG 9,0 66127452
966660 /shared/GeoIP/F5GeoIPRegion2.dat
gtmd 5871 root mem REG 9,0 567630 3915778
/shared/GeoIP/F5GeoIPv6.dat
gtmd 5871 root mem REG 9,0 194864440
966658 /shared/GeoIP/F5GeoIPOrg.dat
gtmd 5871 root mem REG 9,0 5373413
1376259 /shared/GeoIP/F5GeoIPISP.dat
tmm10612 root mem REG 9,0 66127452
/shared/GeoIP/F5GeoIPRegion2.dat
966660
tmm10612 root mem REG 9,0 567630
/shared/GeoIP/F5GeoIPv6.dat
3915778
tmm10612 root mem REG 9,0 194864440
966658/shared/GeoIP/F5GeoIPOrg.dat
tmm10612 root mem REG 9,4 3993525 80575
/usr/share/GeoIP/F5GeoIPISP.dat
```



Note In this case, TMM has loaded the incorrect database file from **/usr/share/GeoIP/F5GeoIPISP.dat**.

To verify the security context of the database files in the /shared/GeoIP directory at the command line

- At the command prompt, type:

```
ls -Z /shared/GeoIP/
```

If the security context for the F5GeoIPISP.dat file is root:object_r:default_t, which is preventing the system from properly loading the IP geolocation database, the following output will appear similar to the following example:

```
lrwxrwxrwx root root root:object_r:shared_geoip_t F5GeoIP.dat -> /
shared/GeoIP/F5GeoIPRegion2.dat
-rw-r--r-- root root root:object_r:default_t F5GeoIPISP.dat
-rw-r--r-- root root system_u:object_r:shared_geoip_t F5GeoIPOrg.dat
-rw-r--r-- root root system_u:object_r:shared_geoip_t F5GeoIPRegion2.
dat
-rw-r--r-- root root system_u:object_r:shared_geoip_t F5GeoIPv6.dat
```

To restore the proper SELinux security context to the geolocation database files

- At the command prompt, type:

```
restorecon -Rv /shared/GeoIP/ ; tmsh load sys geoip
```

BIG-IP Application Security Manager and Deep Packet Inspection signatures

Attack signatures are rules or patterns that identify attack sequences or classes of attacks on a web application and its components. You can apply attack signatures to both requests and responses.

Deep Packet Inspection (DPI) signatures are wrapped up with the BIG-IP ASM signatures. F5 releases a new attack signature update for BIG-IP ASM about every six weeks. The attack signature update includes new attack signatures as well as enhancements to existing attack signatures.

Attack signature updates

Attack signature updates are released only for versions of software that have not yet reached their End of Software Development date, as detailed in AskF5 article: [SOL5903: BIG-IP software support policy](#).

Attack signature updates are available from the [F5 Downloads](#) site (downloads.f5.com), under the version of the BIG-IP system that you are currently running.

Since new web application attacks and threats are constantly being developed, you should update the system-supplied attack signatures on a regular basis to ensure that your applications are protected against new attacks. You can configure automatic



updates, or you can manually update the signatures.

The attack signature updates are cumulative; when you update the system-supplied attack signatures, the update provides the latest signatures and all signatures from the previous updates. Updating the attack signatures also provides any revisions to existing attack signatures.

Attack signatures are also saved in UCS archives. When a UCS archive is created, the current cumulative signature set is saved in the archive. When a UCS archive is restored, the attack signatures in the archive fully replace existing signatures. If the UCS archive is old, the attack signatures may be out-of-date and need to be updated separately.

Attack signature licensing requirements

For the system to initiate the attack signature update, the **Service Check Date** in the BIG-IP ASM system's license must be within 18 months of the system date. If the Service Check Date is recent enough, the system allows the signature update.

If the **Service Check Date** is too old, the BIG-IP ASM system attempts to contact the license server and downloads a new license.

If the system can reach the license server, and the support contract for the system is current: The system downloads a new license and verifies the **Service Check Date**. The system does not install the new license, but only examines it for the required date.

If the **Service Check Date** is within seven days of the system date (accounting for time zone differences and system clock variance) the system initiates the signature update.

If the license server cannot be reached or the support contract for the system is not current, an error message which appears similar to the following example will be reported in the Configuration utility and logged to the `/var/log/asm` file:

```
Service contract cannot be verified (500 read timeout at
/ts/packages//iControl.pm line 1005). Please re-license your installation
of BIG-IP manually. You must manually reactivate the system license and
reinitiate the attack signature update.
```

For more information about the licensing requirements, see AskF5 article: [SOL8217: Updating the BIG-IP ASM attack signatures](#).



Note If the license error persists when attempting to reactivate the license manually, contact F5 Technical Support for questions about the status of the support contract for the affected system.

Configure automatic updates for system-supplied attack signatures

To configure BIG-IP ASM to download the attack signature update files over the Internet you should configure the BIG-IP ASM to download the attack signature update files using either the scheduled update mode or manual update mode. If you select Manual for the Update Mode, you update the attack signatures on your own schedule by clicking **Update Signatures**.



The BIG-IP ASM uses its own self-IP address and default gateway when requesting attack signature updates using the Automatic Method. If Internet access is not available for automatic updates, an error message similar to the following example is reported in the Configuration utility as well as in the `/var/log/asm` file:

```
Signature file server cannot be reached (500 SSL negotiation failed: ).  
Please download the signature file and install manually.
```

To configure BIG-IP ASM to download attack signature updates using scheduled update mode

1. In the Configuration utility, go to **Application Security** and click **Options**.
2. From **Attack Signatures**, click **Attack Signatures Update**.
3. Select **Scheduled**.
4. From **Update Interval** menu, select an update interval.
5. Click **Save Settings**.



Note In version 11.3.0, go to **Security** rather than **Application Security** in step 1.

To configure BIG-IP ASM to download attack signature updates using manual update mode

1. In the Configuration utility, go to **Application Security** and click **Options**.
2. From **Attack Signatures** menu, click **Attack Signatures Update**.
3. Select **Manual**.
4. From **Delivery Mode**, select **Automatic**.
5. Click **Save Settings**.



Note In version 11.3.0, go to **Security** rather than **Application Security** in step 1.



When you are ready to update the attack signatures, click **Check for Updates**, and if an update is available, click **Update Signatures** to download and install the updates.

To configure BIG-IP ASM to use attack signatures from manually downloaded updates

1. Go to the [F5 Downloads](https://downloads.f5.com) page (downloads.f5.com).
2. Manually download the latest signature file to your local workstation.
3. In the Configuration utility, go to **Application Security** and click **Options**.
4. From **Attack Signatures**, click **Attack Signatures Update**.
5. From Update Mode, click **Manual**.
6. From **Delivery Mode**, select **Manual**.
7. Click **Save Settings**.

(Optional) If you want to update the system-supplied signatures now, click **Browse** and go to the previously saved signature file, so that the path to the file appears in the **Upload File** field.

8. Click **Update Signatures** to upload and apply the signature update.



Note Use this option if your BIG-IP ASM system does not have direct Internet access.



If your BIG-IP ASM system is behind a firewall, to allow your system to obtain attack signature updates, you will need to allow access for the following DNS servers and ports:

- Host servers **callhome.f5.com port 443**
- **activate.f5.com port 443** DNS servers

The firewall should allow port 53 access for the DNS name server(s) configured for use by the BIG-IP ASM system.

If the BIG-IP ASM has not been configured with a reachable DNS name server, it will attempt to use an F5 DNS nameserver configured in the **/var/ts/etc/services.ini** file.

The firewall should allow port 53 access for the IP addresses listed for the **prod_dns_server=** setting in this file.

Configure signature file updates through an HTTPS proxy

You can configure the system to use an HTTPS proxy, which allows an administrator to configure the BIG-IP ASM to update attack signatures securely and automatically.

To configure signature file updates through an HTTPS proxy at the command line

1. Change directories to the **/ts/etc/** directory by typing the following command:

```
cd /ts/etc/
```

2. Create a backup of the **services.ini** file by typing the following command:

```
cp services.ini /var/tmp/services.ini.bak
```

3. Using a text editor, add the following section to the end of the **services.ini** file:

```
[proxy] https_proxy=https://<IP address of your HTTPS proxy  
server>:<HTTPS proxy server port>
```

For example:

```
[proxy] https_proxy=https://192.0.2.10:33750
```

4. Save the changes to the **services.ini** file.



Note This change must be made manually on both systems in redundant pair configurations. The **services.ini** file is not copied to the peer system during ConfigSync operations.



EUD

The EUD software is installed with the BIG-IP software on hardware platforms. From time to time, F5 will release updates to the EUD software. For information about the EUD tool and updating the EUD software installed on the BIG-IP system, see [Hardware Diagnostics](#).

Additional resources

The following table points to additional resources you can visit to learn more about the concepts and areas mentioned in this chapter. You can find AskF5 solution articles and the right product manuals for your software version by searching [AskF5 \(support.f5.com\)](#).

Table 9.1: Additional resources

For more information about	See
Phone home.	SOL15000: Using the Automatic Update Check feature.
Security updates.	SOL4602: Overview of the F5 security vulnerability response policy.
Software downloads.	SOL167: Downloading software and firmware from F5.
Transferring file to or from the BIG-IP system.	SOL175: Transferring files to or from an F5 system.
OPSWAT.	SOL10942: Installing OPSWAT hotfixes on BIG-IP APM systems. SOL14207: Determining the active OPSWAT version.
BIG-IP ASM Signature Updates.	SOL8217: Updating the BIG-IP ASM attack signatures. SOL5903: BIG-IP software support policy. SOL9965: The admin user account must be used to license the system.
EUD.	Hardware Diagnostics.

Help improve this guide

Please help F5 improve this guide by responding to a few questions about this chapter.

(Note: You must be viewing this document in Adobe Acrobat Reader or similar to use this form.)

Did this chapter answer all of your questions about the subject matter? Yes No

If not, what information should be included that is not? _____

Did you find any errors pertaining to subject matter in this chapter? Yes No

If yes, please describe the error: _____

If yes, please copy and paste the paragraph containing the error here: _____

Did you find non-subject-matter errors in this chapter (spelling, etc.)? Yes No

If yes, please describe the error: _____

If yes, please copy and paste the paragraph containing the error here: _____



Networking and Cluster Health

At a glance—Recommendations

F5 has identified the following networking and cluster health recommendations:

- Monitor the system (SNMP, Statistics, and AVR) for any changes in normal network performance.
- Follow suggested practices for configuring communication channels between BIG-IP systems in Device Services Clustering High-Availability configurations.
- Configure the BIG-IP system to synchronize its clock with an NTP server.

Background

This section provides context for our recommended procedures in the form of overviews and supplemental information.

Network health

Monitoring network operations on the BIG-IP system and collecting statistical data for use in network traffic analysis are important practices. Information derived from these tasks can provide vital insights into the overall health of your BIG-IP system as a member of your network.

F5 provides several tools for monitoring the status of the BIG-IP system's network functionality.

Statistics dashboard in the Configuration utility

The **Statistics** dashboard, available by going to **Statistics > Dashboard**, provides an overview of critical BIG-IP statistics, such as CPU and memory usage, total connections, SSL transactions per second (TPS), compression, and throughput statistics.

Performance graphs in the Configuration utility

Performance graphs, available by going to **Statistics > Performance**, provides detailed graphs on various BIG-IP system and network statistics.

Snapshots of many of these same performance graphs can also be viewed within BIG-IP iHealth by uploading a qkview file. For more information about qkview files see [BIG-IP iHealth](#).

BIG-IP analytics

BIG-IP Analytics, also known as Application Visibility and Reporting (AVR), is a module for the BIG-IP system, introduced in version 11.0, that lets you analyze performance of web applications. It provides detailed metrics such as transactions per second (TPS), server latency, page load time, request and response throughput, and sessions. You can view metrics for applications, virtual servers, pool members, URLs, specific countries, and additional detailed statistics about an application.



Configuring the AVR module is beyond the scope in this guide. For more information, see [BIG-IP Analytics: Implementations](#) for your software version.

Simple network monitoring protocol

The BIG-IP system also allows for statistics gathering using Simple network monitoring protocol (SNMP), an industry-standard protocol for polling networked devices for statistical data. F5 recommends that you implement some form of SNMP data collection, preferably using a tool to automate, parse, and alert on trending data. Doing so can provide much-needed historical reference into network operations, as well as help identify abnormal traffic patterns that might be indicative of potential problems.

The following list contains information about the core network configuration elements, along with information on how to view the configuration and statistics for each.

Interfaces

Every BIG-IP system includes multiple interfaces. The exact number of interfaces that you have on the BIG-IP system depends on the platform type. For information on BIG-IP platform types, see the appropriate platform guide.

Auto MDI/MDIX behavior for BIG-IP interfaces

An auto MDI/MDIX port detects straight through or crossover Ethernet cable connection types and automatically configures the connection. This behavior eliminates the need for crossover cables when connecting LAN devices. BIG-IP system interfaces support auto MDI/MDIX as follows:

- The BIG-IP system management port (mgmt) supports auto MDI/MDIX. The mgmt port is a special interface dedicated to doing a specific set of system management functions. The MDI/MDIX functionality is retained when you manually configure the Management interface (MGMT) to use specific speed and duplex settings.
- The BIG-IP system's traffic management microkernel (TMM) supports auto MDI/MDIX functionality. MDI/MDIX is retained when you manually configure an interface to use specific speed and duplex settings. You can use either a straight-through cable or a crossover cable when media settings are forced, and you will be able to successfully link to either data terminal equipment (DTE) or data circuit-terminating equipment (DCE) devices.
- The BIG-IP system's TMM switch interfaces are used to send and receive application traffic slated for load balancing. TMM switch interfaces are typically named in the format of "1.1," "1.2," and so on. In the case of VIPRION systems, the blade number will be prepended ("2/1.1", for example). With respect to vCMP guests, the TMM switch interfaces are managed internally by the vCMP hypervisor, and are delineated as "0.x," prepended with the slot ID on VIPRION systems. For example, "1/0.25," "2/0.25," and so on.

For more information, see [BIG-IP TMOS: Concepts](#) for your software version.



Trunks suggested practices

F5 recommends that you assign trunks to VLANs in “tagged” mode (IEEE 802.1q Tagged VLANs) whenever possible. This mode allows each interface to potentially be a member of more than one logical network.

Trunks that are “untagged” are dedicated to the single network segment of the VLAN of which they are a member.

For more information about using Trunks in VLANs, see the [BIG-IP TMOS: Concepts](#) for your software version.

F5 also recommends that on VIPRION Systems, you configure trunks that include interfaces from every blade to ensure traffic is not interrupted in the event of a single blade failure. For more information about VIPRION deployment, see [VIPRION Platform Guide](#).

VLANs

A virtual local area network (VLAN) is a logical subset of hosts on a local area network (LAN) that operate in the same IP address space. Grouping hosts together in a VLAN has distinct advantages.

For example, with VLANs, you can:

- Reduce the size of broadcast domains, thereby enhancing overall network performance.
- Substantially reduce system and network maintenance tasks. Functionally related hosts no longer need to physically reside together to achieve optimal network performance.
- Enhance security on your network by segmenting hosts that must transmit sensitive data.

You can group hosts into VLANs by with the Configuration utility to create a VLAN and associate physical interfaces with that VLAN. As a result, any host that sends traffic to a BIG-IP system interface is logically a member of the VLAN or VLANs to which that interface belongs.

For more information about VLANs, see [BIG-IP TMOS: Concepts](#) for your software version.

VLAN suggested practices

F5 recommends you use VLANs to segregate traffic on different network IP ranges.

When configuring BIG-IP systems in any type of High Availability configuration, F5 recommends configuring a dedicated VLAN for High Availability communications. For more information for VIPRION systems, see AskF5 article: [SOL13915: Configuring network failover for redundant VIPRION systems \(11.x\)](#).

Self IPs

A Self-IP address is an IP address on the BIG-IP system that you associate with a VLAN to access hosts in that VLAN. By virtue of its netmask, a Self-IP address represents a range of IP addresses spanning the hosts in the VLAN, rather than a single host address. You can associate Self-IP addresses not only with VLANs, but also with VLAN groups.



Self-IP addresses serve two purposes:

1. The BIG-IP system uses the Self-IP addresses of its VLANs when sending a message to a destination server to determine the specific VLAN in which a destination server resides.

For example, if a VLAN has a Self-IP address of 10.10.10.100 with a netmask of 255.255.255.0 and the destination server's IP address is 10.10.10.20 with a netmask of 255.255.255.255, the BIG-IP system recognizes that the destination server's IP address falls within the range of VLAN internal's Self-IP address.

Because of this, the BIG IP system sends the message to the interface that you assigned to that VLAN. If more than one interface is assigned to the VLAN, the BIG-IP system takes additional steps to determine the correct interface, such as checking the Layer2 forwarding table.

2. A Self-IP address can serve as the default route for each destination server in the corresponding VLAN. The Self-IP address of a VLAN appears as the destination IP address in the packet header when the server sends a response to the BIG-IP system.

Normally, you will assign Self-IP addresses to a VLAN when you initially run the Setup utility on a BIG-IP system. You assign one static Self-IP address and one floating self- IP address to each of the default VLANs (internal and external). You can later create Self-IP addresses for other VLANs that you create using the Configuration utility.

For more information about Self-IP addresses, see [BIG-IP TMOS: Concepts](#) for your software version.

TMM routes

The BIG-IP system must communicate with other routers, servers, and firewalls in a networked environment. Before you put the BIG-IP system into production, we recommend that you carefully review the router and server configurations in your network. By doing so, you can properly configure routing on the BIG-IP system and adjust the routing configurations on other network devices to include various BIG-IP system IP addresses. Depending on how you configure routing, the BIG-IP system can forward packets to a specified network device (such as a next-hop router or a destination server), or the system can drop packets altogether.

For more information about BIG-IP routing options, see [BIG-IP TMOS: IP Routing Administration](#) for your software version.

ARP

The BIG-IP system supports Address Resolution Protocol (ARP), an industry-standard Layer 3 protocol to find MAC addresses.

The BIG-IP system is a multi-layer network device, and as such, needs to do routing functions. To do this, the BIG-IP system must be able to find destination MAC addresses on the network, based on known IP addresses.

For more information about BIG-IP system's use of ARP, see [BIG-IP TMOS: IP Routing Administration](#) for your software version.



Management IPs and routing

Every BIG-IP system has a management port (mgmt). The management port is a special interface that the BIG-IP system uses to receive or send certain types of administrative traffic.

You cannot use the management port for normal traffic that is slated for load balancing. Instead, the BIG-IP system uses the TMM switch interfaces for that type of traffic. TMM switch interfaces are those interfaces controlled by the Traffic Management Microkernel (TMM) service.

Configuring the management port of a BIG-IP system means assigning an IP address to the port, supplying a netmask for the IP address, and specifying an IP address for the BIG-IP system to use as a default route. The IP address that you assign to the management port must be on a different network than the Self-IP addresses that you assign to VLANs.



Note Specifying a default route for the management port is only necessary if you intend to manage the BIG-IP system from a node on a different subnet.

For more information about the Management Port, see AskF5 article: [SOL15040: Configuring and displaying the management IP address for the BIG-IP system](#).

For more information about Management Routing, see AskF5 article: [SOL13284: Overview of management interface routing \(11.x\)](#).

Device services clustering / high availability health

When running BIG-IP systems in any type of redundancy scenario, several suggested practices can be followed to help ensure smooth operation between members of a High Availability implementation.

When configuring Network Failover, select Self IPs to use as Failover Unicast Addresses on each unit, and use the Management IP as Failover Multicast Addresses on each unit. This configuration provides redundant communication channels over separate distinct network segments to ensure that a failed network link cannot cause an erroneous failover event.

For more information, see AskF5 article: [SOL14135: Defining network resources for BIG-IP, high-availability features \(11.x\)](#).

When configuring BIG-IP systems in any type of High Availability configuration, F5 recommends configuring a dedicated VLAN for High Availability communications.

For more information, see AskF5 article: [SOL13915: Configuring network failover for redundant VIPRION systems \(11.x\)](#).

F5 recommends that you assign static IP addresses to the Management Ports, which ensures consistent ability to access and prevents any possible failover events caused by DHCP offering a different address for the Management Port than expected.

If DHCP must be used, F5 recommends setting up the DHCP server to always assign the same IP address to the BIG-IP Management Port for consistency.



In addition, Device Services Clustering requires that all BIG-IP systems configured into a redundant configuration must use Network Time Synchronization (NTP) to prevent any issues caused by mismatched timestamps between units.

VIPRION systems

On VIPRION systems, F5 recommends that you wire up and configure all Management IPs and routes to allow redundant management access into the system.

Interfaces additional suggested practices

By default, BIG-IP interfaces are configured to auto-negotiate media settings. F5 recommends that you allow this behavior whenever possible. If media settings must be manually set, see AskF5 article: [SOL14107: Configuring the media speed and duplex settings for network interfaces \(11.x\)](#).

F5 recommends that you assign interfaces to VLANs in “tagged” mode (IEEE 802.1q Tagged VLANs) whenever possible. This mode allows each interface to potentially be a member of more than one logical network.

Interfaces that are “untagged” are dedicated to the single network segment of the VLAN of which they are a member.

For more information about using interfaces in VLANs, see [BIG-IP TMOS: Concepts](#) for your software version.

Trunks

A trunk is a logical grouping of interfaces on the BIG-IP system. A trunk increases bandwidth without upgrading hardware and provides link failover if a member link becomes unavailable. You can use trunks to transmit traffic from a BIG-IP system to another vendor switch. Two systems that use trunks to exchange frames are known as peer systems.

When you create a trunk, this logical group of interfaces functions as a single interface. The BIG-IP system uses a trunk to distribute traffic across multiple links, in a process known as link aggregation. With link aggregation, a trunk increases the bandwidth of a link by adding the bandwidth of multiple links together. For example, four fast Ethernet (100 Mbps) links, if aggregated, create a single 400 Mbps link.

With one trunk, you can aggregate a maximum of eight links. For optimal performance, aggregate links in powers of two (two, four, or eight links).

For more information about Trunks, see [BIG-IP TMOS: Concepts](#) for your software version.



Procedures

Follow the procedures detailed in this section to guide you when managing your networks.

View interface configuration

You can view configuration details for the interfaces with the Configuration utility or at the command line.

To view configuration details with the Configuration utility

- Go to **Network > Interfaces > Interface List**.

To view configuration details at the command line

- At the command prompt, type:

```
tmsh list /net interface <interface _ name>
```

View statistics on physical interfaces

You can display information about link status, throughput, errors, and drops for the various interfaces on your platform with the Configuration utility or the command line.

To view the statistics on the physical interfaces from the Configuration utility

1. Go to **Statistics > Module Statistics > Network**.
2. In **Statistics Type**, select to **Interfaces** (default setting).

To view statistics information on the physical interfaces at the command line

- At the command prompt, type:

```
tmsh show /net interface
```

View VLAN configuration information with SNMP

You can configure the BIG-IP system with SNMP traps and an SNMP agent that sends data to an SNMP manager. You can then use the collected data to help you troubleshoot the BIG-IP system.

To view VLAN configuration information through Simple Network Management Protocol (SNMP)

- Go to object identifier:

```
F5-BIGIP-SYSTEM-MIB::sysVlan
```

For more information, see [Monitoring BIG-IP System Traffic with SNMP](#).

View TMM routes configuration

You can view statically configured TMM routes using the Configuration utility or at the command line.

**To view TMM routes configuration using the Configuration utility**

- Go to **Network > Routes**

To view TMM routes configuration at the command line

- At the command prompt, type:

```
tmsh list /net route
```

To view the entire TMM routing table at the command line

- At the command prompt, type:

```
tmsh show /net route
```

View TMM information with SNMP

You can configure the BIG-IP system with SNMP traps and an SNMP agent that sends data to an SNMP manager. You can then use the collected data to help you troubleshoot the BIG-IP system.

To view TMM routes configuration through Simple Network Management Protocol (SNMP)

Go to object identifier:

```
F5-BIGIP-SYSTEM-MIB::sysRoute
```

For more information, see [Monitoring BIG-IP System Traffic with SNMP](#).

View TMM information with SNMP

You can configure the BIG-IP system with SNMP traps and an SNMP agent that sends data to an SNMP manager. You can then use the collected data to help you troubleshoot the BIG-IP system.

To view ARP configuration through Simple Network Management Protocol (SNMP)

- Go to object identifier:

```
F5-BIGIP-SYSTEM-MIB::sysArpNdp
```

For more information, see [Monitoring BIG-IP System Traffic with SNMP](#).

View ARP configuration

You can view configured ARP entries with the Configuration utility or at the command line.

To view statically generated ARP entries with the Configuration utility

- Go to **Network > ARP > Static List**.

To view dynamically generated entries with the Configuration utility



- Go to **Network > ARP > Dynamic List**.

To view statically configured ARP entries at the command line

- At the command prompt, type:

```
tmsh list /net arp
```

ARP monitoring

To view the entire ARP table at the command line

- At the command prompt, type:

```
tmsh show /net arp
```

View IP configuration details

You can view the IP configuration details with the Configuration utility or at the command line.

To view IP configuration with the Configuration utility

- Go to **System > Platform**.

To view IP configuration at the command line

- At the command prompt, type:

```
tmsh list /sys management-ip
```

To view configured management routing at the command line

- At the command prompt, type:

```
tmsh list /sys management-route
```

Monitor IP configuration

To view the management routing table

- At the command prompt, type:

```
ip route show table 245
```

View IP configuration information with SNMP

You can configure the BIG-IP system with SNMP traps and an SNMP agent that sends data to an SNMP manager. You can then use the collected data to help you troubleshoot the BIG-IP system.

To view IP configuration information through Simple Network Management Protocol (SNMP)

- Go to object identifier:



```
F5-BIGIP-SYSTEM-MIB::sysAdminIp
```

For more information, see [Monitoring BIG-IP System Traffic with SNMP](#).

View Self-IP configuration

You can view the configuration details with the Configuration utility or at the command line.

To view network configuration with the Configuration utility

- Go to **Network > Self IPs**

To view network configuration at the command line

- At the command prompt, type:

```
tmsh list /net self
```

View Self-IP configuration information with SNMP

You can configure the BIG-IP system with SNMP traps and an SNMP agent that sends data to an SNMP manager. You can then use the collected data to help you troubleshoot the BIG-IP system.

To view Self-IP configuration information through Simple Network Management Protocol (SNMP)

- Go to object identifier:

```
F5-BIGIP-SYSTEM-MIB::sysSelfIps
```

For more information, see [Monitoring BIG-IP System Traffic with SNMP](#).

View interface information with SNMP

You can configure the BIG-IP system with SNMP traps and an SNMP agent that sends data to an SNMP manager. You can then use the collected data to help you troubleshoot the BIG-IP system.

To view interface information through Simple Network Management Protocol (SNMP)

- Go to object identifier:

```
F5-BIGIP-SYSTEM-MIB::sysInterfaces
```

For more information, see [Monitoring BIG-IP System Traffic with SNMP](#).

View VLAN configuration details

You can view VLAN configuration details with the Configuration utility or at the command line:

To view VLAN configuration details with the Configuration utility

- Go to **Network > VLANs > VLAN List**.

**To view configuration at the command line**

- At the command prompt, type:

```
tmsh list /net vlan
```

To view statistics information for the interfaces assigned to the VLAN on the command line

- At the command prompt, type:

```
tmsh show /net vlan
```

To configure Network Failover with the Configuration utility

- Go to **Device Management > Devices > Device Connectivity > Network Failover**.

View trunk details

If you have configured trunks, you can view the configuration details with the Configuration utility or the command line.

To view trunk details with the Configuration utility

- Go to **Network > Trunks > Trunk List**.

To view trunk details at the command line

- At the command prompt, type:

```
tmsh list /net trunk
```

Monitor trunks

You can view information about link status, throughput, errors and drops for trunks on your platform. You can view these statistics with the Configuration utility or at the command line.



Note vCMP guests inherit VLAN tags from the vCMP hypervisor, so there is no way for guest admins to manage guest VLAN tags directly.

To view trunk statistics with the Configuration utility

1. Go to: **Statistics > Module Statistics > Network**.
2. In **Statistics Type**, select **Trunks**.

To view trunk statistics at the command line

- At the command prompt, type:

```
tmsh show /net trunk
```



View trunks information with SNMP

You can configure the BIG-IP system with SNMP traps and an SNMP agent that sends data to an SNMP manager. You can then use the collected data to help you troubleshoot the BIG-IP system.

To view trunks information through Simple Network Management Protocol (SNMP)

- Go to object identifier:

```
F5-BIGIP-SYSTEM-MIB::sysTrunks
```

For more information, see [Monitoring BIG-IP System Traffic with SNMP](#).

Configure the BIG-IP system to synchronize its clock with an NTP server

F5 recommends configuring the BIG-IP system to synchronize its clock with an NTP server. You can use the tmsh utility to modify or list the NTP settings, as appropriate, for your installation. To do so, configure the BIG-IP system to use an NTP server, list the NTP servers configured on the BIG-IP system, or remove the NTP server configuration.

To configure the BIG-IP system to use an NTP server using tmsh at the command line

- Log in to the Traffic Management Shell (tmsh) utility by typing the following command:

```
tmsh
```

- Configure one or more NTP servers for the BIG-IP system using the following command syntax:

```
modify /sys ntp servers add {hostname hostname....}
```

or

```
modify /sys ntp servers add {ip _ addr ip _ addr....}
```

For example, to add NTP servers with the 192.168.1.245 and 192.168.1.246 IP addresses, type the following command:

```
modify /sys ntp servers add {192.0.2.5 192.0.2.6}
```

- Save the change by typing the following command:

```
save /sys config
```

Verify NTP peer server communications

To use the ntpq utility to query the NTP server and print a summary of the NTP server's state

- At the command prompt, type:

```
ntpq -np
```

The command returns the following fields:



Table 10.1: Ntpq command returns

Field	Definition
prefix to the remote field	<p>An asterisk ({*}) character indicates that the peer has been declared the system peer and lends its variables to the system variables.</p> <p>A plus sign (+) indicates that the peer is a survivor and a candidate for the combining algorithm.</p> <p>A space, x, period (.), dash (), or hash (#) character indicates that this peer is not being used for synchronization because it does not meet the requirements, is unreachable, or is not needed.</p>
remote	The remote field is the address of the remote peer.
refid	<p>The refid field is the Reference ID, which identifies the server, or reference clock with which the remote peer synchronizes, and its interpretation depends on the value of the stratum field (explained in the st definition).</p> <p>For stratum 0 (unspecified or invalid), the refid is an ASCII value used for debugging. Example: INIT or STEP. For stratum 1 (reference clock), the refid is an ASCII value used to specify the type of external clock source. Example: NIST refers to NIST telephone modem. For strata 2 through 15, the refid is the address of the next lower stratum server used for synchronization.</p>
st	<p>The st field is the stratum of the remote peer. Primary servers (servers with an external reference clock such as GPS) are assigned stratum 1. A secondary NTP server, which synchronizes with a stratum 1 server, is assigned stratum 2. A secondary NTP server, which synchronizes with a stratum 2 server, is assigned stratum 3.</p> <p>Stratum 16 is referred to as “MAXSTRAT,” is customarily mapped to stratum value 0, and therefore indicates being unsynchronized. Strata 17 through 255 are reserved.</p>
t	The t field is the type of peer: local, unicast, multicast, or broadcast.
when	The when field is the time since the last response to a poll was received (in seconds).
poll	The poll field is the polling interval (in seconds). This value starts low (example: 64) and over time, as no changes are detected, this polling value increases incrementally to the configured max polling value (example: 1024).
reach	The reach field is the reachability register. The octal shift register records results of the last eight poll attempts.
delay	The delay field is the current estimated delay; the transit time between these peers in milliseconds.
offset	The offset field is the current estimated offset; the time difference between these peers in milliseconds.
jitter	The jitter field is the current estimated dispersion; the variation in delay between these peers in milliseconds.



If the local `ntpd` process fails to communicate with a peer NTP server, the output from the `ntpq` command will appear similar to the following example:

```
#ntpq -np
```

remote	refid	st	t	when	poll	reach	delay	offset	jitter
192.0.2.13	.INIT.	16	u64	0	0.000	0.000	0.000	0000.00	++

In the previous example, the remote server information (refid, stratum, delay, offset, and jitter) is not available. The value `.INIT.` in the refid column indicates that NTP is initializing, and the server has not yet been reached. The value of 0 (zero) in the reach column indicates that the server has not been reached during any of the last eight attempts. The absence of a value in the when column indicates that no data has been received from the remote peer since the local `ntpd` process was started. The poll value of 64 is still at the MINPOLL value, which indicates that NTP was recently restarted.

NTP has a MINPOLL and MAXPOLL value, which it uses to determine the optimal time between updates with the reference server. If jitter is low, and there are no changes in data received, NTP automatically incrementally increases the poll value until it reaches MAXPOLL, or 1024 seconds.

If the local `ntpd` process can communicate or attempts to communicate with a declared peer NTP server, the output from the `ntpq` command appears similar to the following example:

```
#ntpq -np
```

remote	refid	st	t	when	poll	reach	delay	offset	jitter
192.0.2.13	.10.10.10.2514.	2514	u	482	1024	377	0.815	10.010	0.345

In the previous example, the remote server information (refid, stratum, delay, offset, and jitter) displays, which indicates that the servers are successfully exchanging information. The value of 377 in the reach column indicates that the server is successfully reached during each of the last eight attempts, and the value of 482 in the when column indicates that the last response was received from the remote peer 482 seconds ago, which is within the polling interval of 1024 seconds.

Troubleshoot NTP connectivity

If the system is unable to establish communication with the configured remote peer NTP server, you can do the following actions to verify network connectivity:

- Ensure that no firewall rules prevent access to the remote NTP server.
- Ensure that locally-managed time servers are functioning properly.
- Restart the NTP daemon by typing the following command:

```
tmsh restart /sys service ntpd
```

**To list the NTP servers configured on the BIG-IP system at the command line**

1. Log in to the Traffic Management Shell (tmsh) utility by typing the following command:

```
tmsh
```

2. List the NTP servers that are currently defined on the BIG-IP system by typing the following command:

```
list /sys ntp servers
```

To remove the NTP server configuration at the command line

1. Log in to the Traffic Management Shell (tmsh) utility by typing the following command:
2. tmsh
3. Remove the NTP servers that are currently defined on the BIG-IP system by typing the following command:

```
modify /sys ntp servers none
```

4. Save the change by typing the following command:

```
save /sys config
```

Additional resources

The following table points to additional resources you can visit to learn more about the concepts and areas mentioned in this chapter. You can find AskF5 solution articles and the right product manuals for your software version by searching [AskF5](#) (support.f5.com).

Table 10.2: Additional resources

For more information about	See
NTP configurations.	SOL3122: Using the BIG-IP Configuration utility to add an NTP server.

Help improve this guide

Please help F5 improve this guide by responding to a few questions about this chapter.

(Note: You must be viewing this document in Adobe Acrobat Reader or similar to use this form.)

Did this chapter answer all of your questions about the subject matter? Yes No

If not, what information should be included that is not? _____

Did you find any errors pertaining to subject matter in this chapter? Yes No

If yes, please describe the error: _____

If yes, please copy and paste the paragraph containing the error here: _____

Did you find non-subject-matter errors in this chapter (spelling, etc.)? Yes No

If yes, please describe the error: _____

If yes, please copy and paste the paragraph containing the error here: _____



Log Files and Alerts

At a glance—Recommendations

F5 has identified the following log file and alerts recommendations:

- Check available log files for messages pertaining to system stability and health.
- Configure logging to a remote log server(s).
- Review log files to identify and prevent excessive logging.
- Check debug modes to identify excessive logging.
- Configure SNMP traps.

Background

This section provides context for our recommended procedures in the form of overviews and supplemental information, including the following topics:

- BIG-IP system logging.
- Send BIG-IP logs to a remote system.
- Causes of excessive logging.
- Security Information and Event Management.
- Custom SNMP traps.

BIG-IP system logging

Viewing and managing log messages are an important part of maintaining your BIG-IP system. Log messages inform you on a regular basis of the events that are happening on the system. Some of these events pertain to general events happening within the operating system, while other events are specific to the BIG-IP system, such as the stopping and starting of BIG-IP system services.

You can log events either locally on the BIG-IP system or remotely by configuring a remote syslog server using tmsh or using the High-Speed Logging (HSL) mechanism. F5 recommends that you store logs on a pool of remote logging servers using HSL.

For local logging, the HSL mechanism can store the logs in either the syslog or the MySQL database on the BIG-IP system, depending on the destination you define. For remote logging, the HSL mechanism sends log messages to a pool of logging servers that you define.

The mechanism the BIG-IP system uses to log events is the Linux utility syslog-ng. This utility is an enhanced version of the standard UNIX and Linux logging utility syslog.



The types of events that the BIG-IP system logs are:

- System events are based on Linux events, and are not specific to the BIG-IP system.
- Packet filter events are those that result from the implementation of packet filters and packet-filter rules.
- Local traffic events pertain specifically to the local traffic management system.
- Audit events are those that the BIG-IP system logs as a result of changes to the BIG-IP system configuration. Logging audit events is optional.

Logging features

The logging mechanism on a BIG-IP system includes several features designed to keep you informed of system events in the most effective way possible.

You can log different types of events, ranging from Linux system events to packet filtering events to local traffic events. Through the BIG-IP system auditing feature, you can also track and report changes that users make to the BIG-IP system configuration, such as adding a virtual server or designating a device to be part of a redundant system.

When setting up logging on the BIG-IP system, you can customize the logs by designating the minimum severity level or log level at which you want the BIG-IP system to report when a type of event occurs. The possible security levels, from least to most severe are Debug, Informational, Notice, Warning, Error, Critical, Alert, and Emergency. Not all security level options are available for each type of event. Whatever your setting, the system will log events at or more severe than what you set.

For example, if you specify Warning for the logging level when a user makes to the bigdb database, the BIG-IP system will log Warning and more severe messages such as Error and Critical messages, but not less severe ones such as Notice, Informational, or Debug messages.

View logs

You can use the Configuration utility to search for a string within a log event, that is, filter the display of the log messages according to the string you provide.

You can view historical logs using the Traffic Management shell (tmsh). For more information, see the [Traffic Management Shell \(tmsh\) Reference Guide](#).

You can log BIG-IP system events to a remote logging server. You do this by identifying the IP address or host name of the remote logging server, and creating an encrypted network connection, or tunnel, for sending log information to that remote server.



Tip You can also configure the system to send email or activate pager notification based on the priority of the logged event.



Log content

The logs that the BIG-IP system generates include several types of information. For example, some logs show a timestamp, host name, and service for each event. Logs sometimes include a status code, while the audit log shows a user name and a transaction ID corresponding to each configuration change. All logs contain a one-line description of each event.

The following table lists the categories of information contained in the logs and the specific logs in which the information is displayed.

Table 11.1: Log information categories and their descriptions

Information type	Explanation	Log type
Timestamp.System	The time and date that the system logged the event message.	Packet Filter, Local Traffic, Audit.
Host name	The host name of the system that logged the event message. Because this is typically the host name of the local machine, the appearance of a remote host name could be of interest.	System, Packet Filter, Local Traffic.
Service	The service that generated the event.	System, Packet Filter, Local Traffic.
Status code	The status code associated with the event. Note that only events logged by BIG-IP system components, and not Linux system services, have status codes.	Packet Filter, Local Traffic.
Description	The description of the event that caused the system to log the message.	System, Packet filter, Local traffic.
User name	The name of the user who made the configuration change.	Audit.
Transaction ID	The identification number of the configuration change.	Audit.
Event	A description of the configuration change that caused the system to log the message.	Audit.

Local syslog logging

If you are using the syslog utility for local logging, whether or not you are using the high-speed logging mechanism, you can view and manage the log messages, using the BIG-IP Configuration utility.



The local syslog logs that the BIG-IP system can generate include several types of information. For example, some logs show a timestamp, host name, and service for each event. Logs sometimes include a status code, while the audit log shows a user name and a transaction ID corresponding to each configuration change. All logs contain a one-line description of each event. For local log messages that the BIG-IP system stores in the local syslog database, the BIG-IP system automatically stores and displays log messages in these categories:

- System messages packet filter messages.
- Local Traffic messages.
- Global Traffic messages.
- BIG-IP system configuration (audit) messages.

Each type of event is stored locally in a separate log file, and the information stored in each log file varies depending on the event type. All log files for these event types are in the **directory /var/log**.

Logging system events

Many events that occur on the BIG-IP system are Linux-related events, and do not specifically apply to the BIG-IP system. Using the Configuration utility, you can display these local system messages. The system logs the messages for these events in the **/var/log/messages** file.

Logging packet filter events

Some of the events that the BIG-IP system logs are related to packet filtering. The system logs the messages for these events in the **/var/log/pktfilter** file.

Logging local traffic events

Many of the events that the BIG-IP system logs are related to local area traffic passing through the BIG-IP system. The BIG-IP system logs the messages for these events in the **/var/log/ltn** file.

Logging of BIG-IP system configuration (audit) events

The BIG-IP system logs the messages for these events in the **/var/log/audit** file.

Manage logging levels

The BIG-IP system uses the standard UNIX logging utility, syslog-ng, to deliver system messages to log files. You can configure the level of information that syslog-ng delivers to log files.



Note Log messages for events related to Traffic Management Microkernel (TMM) are controlled by the alertrd process. For detailed information about configuring the level of information logged for TMM events see AskF5 article: [SOL5532: Configuring the level of information logged for TMM specific events.](#)

Syslog-ng uses facilities and levels to describe system messages. Facilities describe the specific element of the system generating the message. Levels describe the severity of the message.

Facilities

The following facilities are available on the BIG-IP system. Each facility handles messages for specific elements of the system:

Table 11.2: Available facilities

Facility	Description	Default log file
local0	BIG-IP specific messages.	<code>/var/log/ltm</code>
local1	EM specific messages	<code>/var/log/em</code>
	BIG-IP APM specific messages.	<code>/var/log/apm</code>
local2	BIG-IP DNS and BIG-IP Link Controller specific messages.	<code>/var/log/gtm</code>
local3	BIG-IP ASM specific messages.	<code>/var/log/asm</code>
local4	ITCM portal and server (iControl) specific messages.	<code>/var/log/ltm</code>
local5	Packet Filtering specific messages.	<code>/var/log/pktfilter</code>
local6	HTTPD specific messages.	<code>/var/log/httpd/httpd_errors</code>
local7	Linux specific boot messages.	<code>/var/log/bootlog</code>
cron	Messages related to the cron daemon.	<code>/var/log/cron</code>
daemon	Messages related to system daemons (including named and ntpd).	<code>/var/log/daemon.log</code>
kern	Kernel messages.	<code>/var/log/kern.log</code>
mail	Mail system messages.	<code>/var/log/maillog</code>
auth	User authentication messages that do not contain sensitive information.	<code>/var/log/secure</code>
authpriv	User authentication messages that contain sensitive information.	<code>/var/log/secure</code>
ftp	Unused, messages for FTP are reported under daemon.	N/A
lpr	Unused, printing support is not provided.	N/A
mark	A facility that produces time-stamps at regular intervals.	N/A
news	Unused, news server support is not provided.	N/A
ntp	Unused, messages for ntpd are reported under daemon.	N/A
user	Messages related to user processes.	<code>/var/log/user.log</code>



Facility	Description	Default log file
uucp	Unused.	None

Levels

The following levels are available for each facility, as described in the following table. The facilities are listed in order of the severity of the messages they handle. Generally, higher levels contain all the messages for lower levels. For example, the alert level will generally also report all messages from the emerg level, and the debug level will generally report all messages for all levels.

Table 11.3: Emerg level report messages

Level	Description	Verbosity
emerg	Emergency system panic messages.	Minimum
alert	Serious errors that require administrator intervention.	Low
crit	Critical errors, including hardware and filesystem failures.	Low
err	Non-critical, but possibly very important, error messages.	Low
warning	Warning messages that should at least be logged for review.	Medium
notice	Messages that contain useful information, but may be ignored.	Medium
info	Messages that contain useful information, but may be ignored.	High
debug	Messages that are only necessary for troubleshooting.	Maximum



Note The BIG-IP system is not a logging server and has limited capacity for storing, archiving, and analyzing logs. A dedicated logging server is recommended for extensive logging functions. The BIG-IP system is configured by default to provide the most relevant log information to administrators.



Changing the default log levels to a higher level will increase the amount of data stored on the device. If the default levels are changed for troubleshooting purposes, remember to set the level back to its default setting.

Display the level of information that syslog-ng sends to log files

Before you change a specific syslog facility level, you may want to display the current levels.

Procedures

Follow the procedures detailed in this section to guide you when managing your networks.

SysLog

To display the current syslog facility levels

1. Log in to the Traffic Management Shell (tmsh) at the command line by typing the following command:

```
tmsh
```

2. Change to the **/sys** module by typing the following command:

```
/sys
```

3. To list the level of information that syslog-ng sends to the log files, type the following command:

```
list syslog all-properties
```

To configure the level of information, syslog-ng sends to log files

1. Log in to the Traffic Management Shell (tmsh) at the command line by typing the following command:

```
tmsh
```

2. Change to the **/sys** module by typing the following command:

```
/sys
```

3. Use the following syntax to modify the level of information that syslog-ng sends to log files:

```
modify syslog <option>
```

For example, the default log level range for the authpriv syslog facility is from notice to emerg.

4. To change the authpriv syslog facility range from warning to emerg, type the following command:

```
modify syslog auth-priv-from warning
```



Note For other syslog options, use the **help /sys syslog** command from the tmsh shell.



5. Save the change by typing the following command:

```
save sys config
```

Manage log files on the BIG-IP system

Log files allow one to track usage or troubleshoot issues. If left unmanaged, they can grow to an unwieldy size. The BIG-IP system uses a utility called logrotate to manage the local log files. The default settings will suffice for most systems. If it is determined that the current system is logging at a high level, the following sections will describe how to modify the default settings.

Change the age at which log files become eligible for removal

The logrotate script deletes log files older than the number of days specified by the Logrotate.LogAge database variable. By default, the variable is set to 8. Therefore, the system is configured to delete archive copies that are older than eight days.

To modify the Logrotate.LogAge database variable

1. Log in to the Traffic Management Shell (tmsh) at the command line by typing the following command:

```
tmsh
```

2. Modify the age at which log files are eligible for deletion, by using the following command syntax:

```
modify /sys db logrotate.logage value <value>
```

In this command syntax, note the following: Legal values range from 0 to 100

3. Save the change by typing the following command:

```
save /sys config
```

Change the number of archive copies that the system retains

The tmsh log-rotate common-backlogs option specifies the maximum number of log files that the system retains for each log file. By default, the BIG-IP system is configured to retain up to a maximum of 24 archive copies of each log file.



Note The system is unlikely to reach the maximum of 24 archive copies for a log file unless you change the log rotation frequency or the Logrotate.LogAge database variable.

**To modify the number of archived log files**

1. Log in to the Traffic Management Shell (tmsh) at the command line by typing the following command:

```
tmsh
```

2. Modify the number of archived logs that the system retains by using the following command syntax:

```
modify /sys log-rotate common-backlogs <value>
```

In this command syntax, note the following: Legal values range from 0 to 100.

3. Save the changes at the command prompt, type:

```
save /sys config
```

Send BIG-IP logs to a remote system

You can log events locally on the BIG-IP system or remotely by configuring a remote syslog server using tmsh or using the BIG-IP system's High-Speed Logging (HSL) mechanism.

To configure a remote syslog system at the command line

1. At the command prompt, type syntax:

```
modify /sys syslog remote-servers add {<server name> {host <server IP  
address> remote-port <port number>}}
```

For example:

```
modify /sys syslog remote-servers add {server{host 10.1.1.1 remote-port  
514}}
```

Changes made with the **tmsh syslog** commands must be saved in order to persist after a configuration reload.

2. To save changes at the command prompt, type:

```
save /sys config
```

For more advanced configurations, like sending logs to multiple remote syslog servers, see AskF5 article: [SOL13080: Configure the BIG-IP system to log to a remote syslog server \(11.x\)](#).

To implement high-speed remote logging of BIG-IP system processes, see [Configuring Remote High-Speed Logging](#) in the [BIG-IP TMOS: Implementations Guide](#) for the software version you are running.

Configure remote logging v. remote high-speed logging configuration

If you want to configure remote logging using syslog-ng, do not use high-speed logging (HSL). Configuration of remote logging using syslog-ng has some key differences compared to a remote, HSL configuration.

You do not configure log destinations, publishers, or a logging profile or log filter. Instead of creating a pool of remote logging servers (as you do with high-speed logging), specify the IP addresses of the servers using the **Remote Logging** page of the BIG-IP Configuration utility. If you want to ensure that the syslog-ng messages being logged remotely are encrypted, you must first establish a secure tunnel.

Examples of the types of messages that the HSL mechanism can log are: BIG-IP system-level events DNS events (for local traffic and global traffic) Network Firewall events

Protocol Security Manager™ events carrier-grade NAT (CGNAT) events Distributed Denial of Service (DDoS) protection events

To set up remote HSL first define a pool of logging servers, and then create an unformatted, remote high-speed log destination that references the pool. If you are using ArcSight, Splunk, or Remote Syslog logging servers that require a formatted destination, you can also create a formatted log destination for one of those server types. Once those objects are set up, you create a publisher and a custom logging profile pertaining to the type of message you want to log. You then assign the logging profile to a relevant virtual server, and the profile, in turn, references the publisher. The following figure shows BIG-IP objects that you configure for remote high-speed logging. The figure shows the way that these objects reference one another from a configuration perspective.

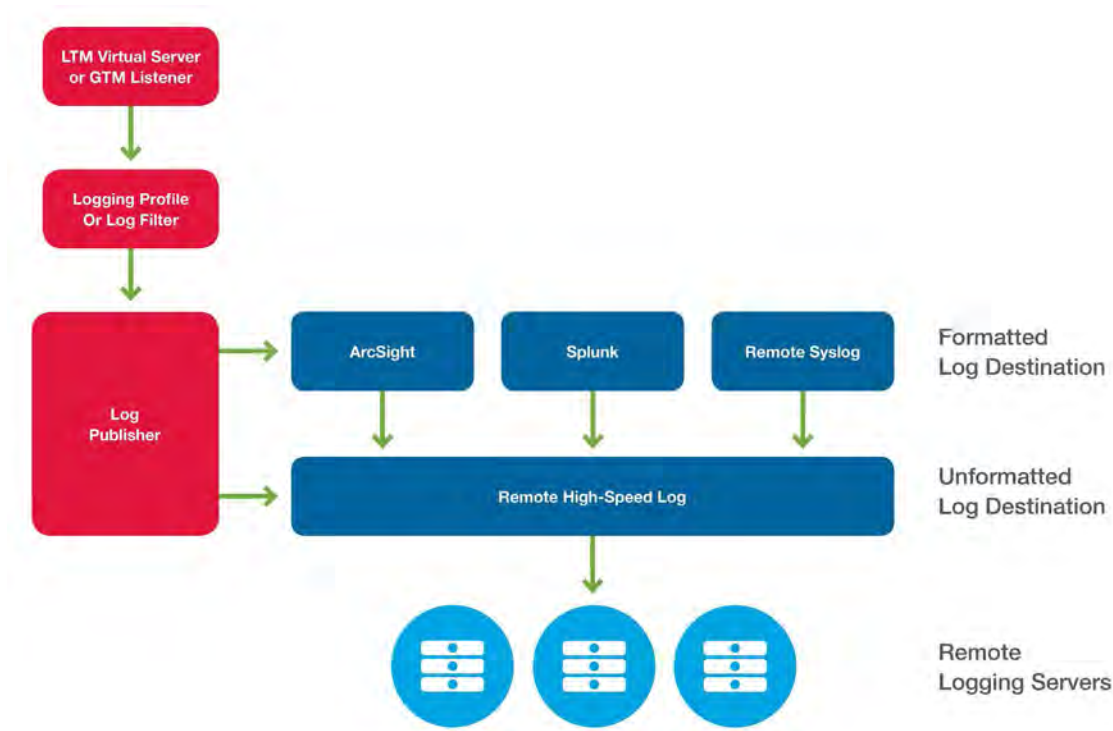


Figure 11.1 BIG-IP objects configured for remote high-speed logging

**Table 11.4: Description of high-speed logging configuration objects**

Configuration object	Description
Remote logging pool	A remote logging pool is a BIG-IP load balancing pool that contains the remote logging servers as members.
Unformatted log destination	An unformatted log destination references the pool of remote logging servers.
Formatted log destination	A formatted log destination pertains to a specific type of remote logging server (ArcSight, Splunk, or Remote Syslog) and references an unformatted log destination.
Log publisher	A log publisher references the formatted and unformatted log destinations for log messages.
Logging profile	A logging profile pertains to the type of events that you want to log. For example, for logging Protocol Security events, you create a Protocol Security logging profile. For Network Firewall events, you create a Network Firewall profile. A logging profile references a log publisher.
Log filter	A log filter is a mechanism for setting minimum log levels for various system-level events. A log filter references a log publisher.
BIG-IP LTM virtual server or BIG-IP DNS listener	A virtual server or listener listens for the type of traffic for which you want to log messages. If you have created a logging profile, you assign the profile to the virtual server or listener.

Example: In configuring a remote, high-speed logging, you want to send all Protocol Security messages to a group of remote ArcSight servers. You create the following:

- A load balancing pool for the ArcSight logging servers.
- An unformatted Remote High-Speed Log destination that references the pool of ArcSight logging servers.
- A formatted ArcSight log destination that references an unformatted log destination.
- A publisher that references the formatted and unformatted log destinations.
- A Protocol Security logging profile that references the publisher.
- A BIG-IP LTM virtual server or DNS listener that references the logging profile and the load balancing pool.
- An unformatted Remote High-Speed Log destination that references the pool of ArcSight logging servers.



Tip For step-by-step information on configuring basic remote high-speed logging, see [BIG-IP TMOS: Implementations](#).



Audit logging

Audit logging is an optional type of logging which logs messages pertaining to configuration changes that users or services make to the BIG-IP system configuration. This type of audit logging is known as master control program (MCP) audit logging. Optionally, you can set up audit logging for any tmsh commands that users type on the command line.

For both MCP and tmsh audit logging, you can choose a log level. In these types of logging, log levels do not affect the severity of the log messages. Instead, the log levels affect the initiator of the audit event.

The log levels for MCP logging are described in the following table.

Table 11.5: MCP logging levels

Level	Description
Disable	Turns off audit logging (Default).
Enable	Causes the system to log messages for user- initiated configuration changes only.
Verbose	Causes the system to log messages for user- initiated configuration changes and any loading of configuration data.
Debug	Causes the system to log messages for all user- initiated and system-initiated configuration changes.

The log levels for tmsh logging are described in the following table.

Table 11.6: tmsh logging levels

Level	Description
Disable	Turns off audit logging (Default).
Enable	Causes the system to log messages for user- initiated configuration changes only.



Causes of excessive logging

A variety of things can cause excessive logging. Among these are iRules logging functionality and debug modes.

iRules

Logging functionality within iRules can cause excess logging to the system. F5 recommends you check system log load after editing or adding iRules.

Debug modes

Depending on the level of debug information turned on in debug mode, significant impact on the system CPU load may result. See AskF5 article: [SOL13455: Overview of BIG-IP logging BigDB database keys \(11.x\) for an overview of BIG-IP database keys that control debug logging](#).

Security information and event management

Security Information and Event Management (SIEM) is a term for software and products services combining security information management (SIM) and security event manager (SEM). SIEM can centralize the storage and interpretation of logs, or events, generated by software running on the network. As a network security device, the BIG-IP device can be configured to send log data and SNMP traps to a SIEM device to help provide real-time analysis of security events and generate reports for compliance purposes.

You can configure the BIG-IP system to log information about protocol security, network firewall, and denial-of-service (DoS) events and send the log messages to remote high-speed log servers.



Important The BIG-IP Advanced Firewall Manager™ (AFM™) must be licensed and provisioned before you can configure DoS protection, network firewall and protocol security event logging. Additionally, for high-volume logging requirements, such as DoS, ensure that the BIG-IP system sends the event logs to a remote log server.



See the following chapters in [External Monitoring of BIG-IP Systems: Implementations Guide](#) for the software version you are currently running:

- [Configuring Remote High-Speed Logging of Protocol Security Events.](#)
- [Configuring Remote High-Speed Logging of Network Firewall Events.](#)
- [Configuring Remote High-Speed Logging of DoS Protection Events.](#)

BIG-IP ASM allows administrators to configure a remote logging profile to send request data for an associated web application to a remote system such as Splunk or ArcSight. A remote management system allows an administrator to store data in a central location for multiple appliances/applications for archival and reporting purposes.

For more information about configuring the remote-logging profile for use with remote management systems, see Configuration Guide for BIG-IP Application Security Manager for your software version.

For more information about ArcSight Remote Logging with BIG-IP ASM, see AskF5 article: [SOL11995: Data field definitions for ArcSight Remote Logging.](#)

For information on reporting and analytics for Splunk, see the following Splunk Apps at <http://apps.splunk.com> (This link takes you to an outside resource.):

- Splunk for F5 is a collection of field extractions, saved searches, reports dashboards, and web access iRules for BIG-IP Local Traffic Manager.
- Splunk for F5 Access is a collection of field extractions, saved searches, reports, and dashboards for BIG-IP Access Policy Manager and FirePass™ SSL VPN.
- Splunk for F5 Security is a collection of field extractions, saved searches, reports, and dashboards for BIG-IP Access Security Manager and Protocol Security Manager

Custom Simple Network Management Protocol traps

Simple Network Management Protocol (SNMP) traps are definitions of unsolicited notification messages that the BIG-IP alert system and the SNMP agent send to the SNMP manager when certain events occur on the BIG-IP system. Configuring SNMP traps on a BIG-IP system means configuring how the BIG-IP system handles traps, as well as setting the destination to which the notifications are sent.

All BIG-IP systems are pre-configured with a set of trap definitions which are helpful for managing the hardware and software components of the device. In most cases, default traps are sufficient for monitoring and managing the system. However, some deployments require custom SNMP traps on other logged events.

The BIG-IP system uses a standard **syslog-ng / alertrd** framework for generating alerts, including SNMP traps. SNMP traps are triggered when the alertrd process receives input from the syslog-ng utility that matches an alert code or match string. The



alrtd process then does the action specified in the **/etc/alrtd/alert.conf** or **/config/user_alert.conf** file, such as sending an SNMP trap.

Before you attempt to define a custom SNMP trap, you should already have SNMP configured on the BIG-IP system with at least one trapsink destination. If not, see *External Monitoring of BIG-IP Systems Implementation Guide* for your software version.

The BIG-IP system stores SNMP traps in two specific files:

- **/etc/alrtd/alert.conf**, which contains default SNMP traps.
- **/config/user_alert.conf**, which Contains user-defined SNMP traps.



Important Do not add or remove traps from the **/etc/alrtd/alert.conf** file.

F5 does not recommend or support modifications to the **/etc/alrtd/alert.conf** file. The **/etc/alrtd/alert.conf** file is not stored in UCS archives, and it may be overwritten during hotfix installations and software upgrades. All custom alerts should be defined in the **/config/user_alert.conf** file.

For information about determining the format of the syslog-ng message strings sent with an SNMP trap, see AskF5 article: [SOL6420: The /var/run/bigip_error_maps.dat file maps the alrtd process input from the syslog-ng utility to an alert name.](#)

SNMP trap definitions

You can determine which alerts will trigger an SNMP trap by viewing **/etc/alrtd/alert.conf**. The **/etc/alrtd/alert.conf** file contains the alert definitions, which instruct the system on what actions to take when the alert is triggered.

An alert definition appears similar to the following example:

```
alert BIGIP _ MCPD _ MCPDERR _ POOL _ MEMBER _ MON _ STATUS
{snmptrap OID="1.3.6.1.4.1.3375.2.4.0.10" }
```

Alert definitions configured to trigger an SNMP trap will contain the snmptrap command, as in the previous example:

```
snmptrap OID="1.3.6.1.4.1.3375.2.4.0.10";
```

The first line always contains the alert name:

```
alert BIGIP _ MCPD _ MCPDERR _ POOL _ MEMBER _ MON _ STATUS
```

The first line of an alert definition may also contain the match string, as in the following example, which uses a regular expression to catch all local authentication failure log messages:

```
alert BIGIP _ AUTH _ FAIL "FAILED LOGIN (.) FROM (.) FOR
(.*), Authentication failure" { snmptrap OID="1.3.6.1.4.1.3375.2.4.0.27" }
```

When the alrtd process starts, the **/var/run/bigip_error_maps.dat** file is dynamically generated using entries from all of the map files in the **/etc/alrtd/** directory that end with the **_maps.h** file extension.



The `alrtd` process uses the `/var/run/bigip_error_maps.dat` file to map input it receives from the `syslog-ng` utility to an alert name. When `alrtd` receives input from `syslog-ng` utility that matches an alert code, the alert code is mapped to the alert name. The `alrtd` process then does the alert actions specified for that alert name in the `/etc/alrtd/alert.conf` file, such as issuing an LCD warning, or sending an SNMP trap.



Important Modifications to the `/config/user_alert.conf` file may not be preserved after system upgrades or hotfix installations. F5 recommends that you create an updated UCS archive immediately before an upgrade operation if you want to maintain the customizations in the file.

SNMP trap configuration files

Standard pre-configured SNMP traps are contained in the `/etc/alrtd/alert.conf` file. F5 does not recommend or support the addition or removal of traps or any other changes to the `alert.conf` file.

Custom, user-defined SNMP traps should be defined in the `/config/user_alert.conf` file.

When the `alrtd` process starts, it creates a dynamic configuration file by appending the `/config/user_alert.conf` file to the `/etc/alrtd/alert.conf` file. The system searches the dynamic configuration file sequentially for matches. Once a match is found, the trap is generated and no further matches are attempted.

All files in the `/config` directory, including any customizations to the `/config/user_alert.conf` file, are automatically included in the UCS archive by default. For more information, see AskF5 article: [SOL4422: Viewing and modifying the files that are configured for inclusion in a UCS archive](#).

Create custom SNMP traps

Before you create a custom trap, you must determine the unique syslog message(s) for which you want the system to send alerts. The first matched message value will generate an alert, so the message must not match the `matched_message` value of any other SNMP trap already defined in the `/etc/alrtd/alert.conf` file or the `/config/user_alert.conf` file.

For information about how to determine which alerts are pre-configured to trigger an SNMP trap or to view alerts from the `/etc/alrtd/alert.conf` file, see AskF5 article: [SOL6414: Determining which alerts are pre-configured to trigger an SNMP trap](#).

To create a custom SNMP trap at the command line

1. Back up your `/config/user_alert.conf` file by typing the following command:

```
cp /config/user _ alert.conf/config/user _ alert.conf.SOL3727
```

2. Edit the `/config/user_alert.conf` file.

3. Add a new SNMP trap using the following syntax:

```
alert <alert _ name> "<matched message>" { snmptrap OID=".1.3.6.1.4.1.3375.2
.4.0.XXX" }
```



See Custom SNMP trap naming for information on how to name custom traps.

4. Save the file and close the text editor.

Custom SNMP trap naming

When you add a new SNMP trap, use the following syntax:

```
alert <alert_name> "<matched message>" { snmptrap OID=".1.3.6.1.4.1.3375.2.4.0.XXX" }
```

- Replace **XXX** with a number unique to this object ID.
- Replace the **<alert_name>** with a descriptive name. Do not use an alert name that exactly matches one already used in the **/etc/alertd/alert.conf** file or the **/config/user_alert.conf** file.
- Replace the **<matched_message>** with text that matches the syslog message that triggers the custom trap. You can specify a portion of the syslog message text or use a regular expression.

F5 recommends that you do not include the syslog prefix information in the match string, such as the date stamp and process ID. Including information of a variable nature in the match string or regular expression may result in unexpected false positives or result in no matches at all.

You can use any object ID that meets all of the following criteria:

- The object ID (OID) is in standard OID format and within the range .1.3.6.1.4.1.3375.2.4.0.300 through .1.3.6.1.4.1.3375.2.4.0.999
- If the OID value is outside the range listed above, a trap will be sent with the OID specified, but it will not contain any text within the trap body.
- The object ID is in a numeric range that can be processed by your trap receiving tool.
- The object ID does not already exist in the **/usr/share/snmp/mibs/F5-BIGIP- COMMON-MIB.txt MIB** file.
- The object ID is not already used in another custom trap.



Note If the alertd process fails to start, examine the newly added entry to ensure it contains all of the required elements and punctuation.

To test the newly created trap, see AskF5 article: [SQL11127: Testing SNMP traps on BIG-IP \(9.4x-11.x\)](#).



Custom SNMP trap example

When switchboard failsafe is enabled, a message that appears similar to the following example is logged to the `/var/log/ltm` file:

```
Sep 23 11:51:40 bigipl.askf5.com lacpd[27753]: 01160016:6: Switchboard
Failsafe enabled
```

To create a custom SNMP trap that is triggered whenever switchboard failsafe status changes are logged, add the following trap definition to the `/config/user_alert.conf` file:

```
alert SWITCHBOARD _ FAILSAFE _ STATUS "Switchboard Failsafe (.*)"
{
    snmptrap OID=".1.3.6.1.4.1.3375.2.4.0.500"
}
```

Additional resources

The following table points to additional resources you can visit to learn more about the concepts and areas mentioned in this chapter. You can find AskF5 solution articles and the right product manuals for your software version by searching [AskF5 \(support.f5.com\)](https://support.f5.com).

Table 11.7: Additional resources

For more information about	See
Configuring alerts to send email notifications.	SOL3667: Configuring alerts to send email notifications
External monitoring.	External Monitoring of BIG-IP Systems: Implementations
SNMP traps.	Custom SNMP Traps on DevCentral (Login required)
Configuring the level of information that syslog-ng sends to log files (11.x).	SOL13317: Configuring the level of information that syslog-ng sends to log files (11.x)
Configuring the level of information logged for TMM-specific events.	SOL5532: Configuring the level of information logged for TMM-specific events
Configuring syslog settings at the command line (11.x)	SOL13083: Configuring syslog settings at the command line (11.x)

Help improve this guide

Please help F5 improve this guide by responding to a few questions about this chapter.

(Note: You must be viewing this document in Adobe Acrobat Reader or similar to use this form.)

Did this chapter answer all of your questions about the subject matter? Yes No

If not, what information should be included that is not? _____

Did you find any errors pertaining to subject matter in this chapter? Yes No

If yes, please describe the error: _____

If yes, please copy and paste the paragraph containing the error here: _____

Did you find non-subject-matter errors in this chapter (spelling, etc.)? Yes No

If yes, please describe the error: _____

If yes, please copy and paste the paragraph containing the error here: _____



Modules

At a glance—Recommendations

F5 has identified the following module recommendations:

- Determine which modules are system on your BIG-IP system.
- Check pool load balancing statistics and verify pool member availability.
- Ensure ZoneRunner™ configuration matches the BIND configuration files after a BIND restart or crash.
- Check expiration dates of your domain names.
- Reactivate service license to update service check date.
- Test BIG-IP Application Security Manager sync and failover capabilities (High availability configurations only).
- Review attack signatures and policies.
- Review logged violations for accuracy.
- Perform regular penetration testing.
- Set up remote logging for violations.
- Set up Simple Network Management Protocol traps for violations.
- Turn off learning for policies in blocking mode.
- Protect application from DDoS attacks.
- Delay access or drop connections and increase data storage WAN Optimization Manager uses for deduplication if a DDoS attack is suspected.
- Monitor solid state drives use.

Background

This section provides context for our recommended procedures in the form of overviews and supplemental information.

It includes general information on the following BIG-IP system modules:

- BIG-IP DNS (formerly Global Traffic Manager/GTM)
- BIG-IP Local Traffic Manager (LTM)



- BIG-IP Application Firewall Manager (AFM)
- BIG-IP Access Policy Manager (APM)
- BIG-IP Application Security Manager (ASM)
- BIG-IP Application Acceleration Manager™ (AAM™)
- BIG-IP Policy Enforcement Manager™ (PEM™)
- BIG-IP Carrier-Grade NAT BIG-IP Link Controller
- BIG-IP Enterprise Manager (EM)
- BIG-IP Protocol Security Module (PSM)

For more information about the key benefits for each of the F5 modules, see [The BIG-IP Modules Datasheet \(f5.com/pdf/products/big-ip-modules-ds.pdf\)](https://f5.com/pdf/products/big-ip-modules-ds.pdf).

Modules

F5 BIG-IP devices work on a modular system, so you can add new functions as necessary to adapt quickly to changing application and business needs. F5 offers a range of feature modules users can activate on demand. BIG-IP software modules offer advanced security, performance and availability features allowing customization of BIG-IP to your unique data environment.

You can provision modules for which you are not licensed. This enables you to configure the system prior to obtaining a license. If you provision modules without a valid license, the system posts the following alert in the Configuration utility:

```
Provisioned yet unlicensed: <modulename>
```

Although you can provision an unlicensed module, associated modules features will not be operable.



Note Check your license to determine which modules you have activated on your system. Trial licenses, can expire without warning. For more information, see [Licenses and Entitlement](#).



BIG-IP DNS

BIG-IP DNS (formerly Global Traffic Manager/GTM) improves the performance and availability of your applications by directing users to the closest or best-doing physical, virtual, or cloud environment. Using high-performance DNS services, BIG-IP GTM scales and secures your DNS infrastructure from DDoS attacks and delivers a complete, real-time DNSSEC solution that protects against hijacking attacks.

For more information see the [BIG-IP DNS/Global Traffic Manager](https://f5.com/products/modules/global-traffic-manager) product page (f5.com/products/modules/global-traffic-manager).

Wide IP misses/fallback to BIND

BIG-IP DNS attempts to load balance a name resolution request using the preferred load balancing method configured for the pool. If the preferred load-balancing method fails, the system attempts to use the alternate and fallback methods. If all of the load-balancing methods that are configured for a pool fail, then the request fails, or the system falls back to BIND.

Wide IP misses/fallback to BIND may occur for a variety of reasons. For example, a wide IP may fall back to BIND if all pool members are marked down in the pool. In addition, the wide IP may fall back to BIND when an AAAA or A6 query is received by BIG-IP DNS and no IPv6 pool members exist for the wide IP.

ZoneRunner data matches BIND zone files

BIG-IP DNS uses ZoneRunner to manage DNS zone files and the BIND configuration. The ZoneRunner utility uses Dynamic DNS Update to update the resource record data to BIND. BIND does not write the updates to the associated zone file immediately. Instead, it stores the updates in a journal file, with a .jnl file name extension. If BIND is restarted after a shutdown or crash, it replays the journal file and attempts to incorporate the zone data. In the event the replay fails, the ZoneRunner data may not match the BIND files.

Domain name expiration

Once a domain name expires, it goes through many stages before being released to the open market. Most domain name registrars send renewal emails to domain name administrators prior to the expiration date.

BIG-IP Local Traffic Manager

BIG-IP Local Traffic Manager (LTM) increases your operational efficiency and ensures peak network performance by providing a flexible, high-performance application delivery system. With its application-centric perspective, BIG-IP LTM optimizes your network infrastructure to deliver availability, security, and performance for critical business applications. For more information see the [BIG-IP Local Traffic Manager](https://f5.com/products/modules/local-traffic-manager) product page (f5.com/products/modules/local-traffic-manager).



BIG-IP Advanced Firewall Manager

BIG-IP Advanced Firewall Manager (AFM) is a high-performance, stateful, full-proxy network firewall. It is designed to guard data centers against incoming threats that enter the network on the most widely deployed protocols, including HTTP/S, SMTP, DNS, and FTP. By aligning firewall policies with the applications they protect, BIG-IP AFM streamlines application deployment, security, and monitoring. With its scalability, security, and simplicity, BIG-IP AFM forms the core of the F5 application delivery firewall solution.



Note IPFIX is a generic logging capability used by carrier-grade NAT (CGNAT), BIG-IP AFM, and BIG-IP PEM. In terms of transport, you can specify UDP, TCP, or TLS with TCP. If your IP Flow Information Export (IPFIX) collector is capable of TLS, F5 recommends specifying one of these terms of transport as the preferred transport when security is an issue.

BIG-IP Access Policy Manager

BIG-IP Access Policy Manager (APM) is a flexible, high-performance access and security solution that provides unified global access to your applications and network. By converging and consolidating remote access, LAN access, and wireless connections within a single management interface, and providing easy-to-manage access policies, BIG-IP APM helps you free up valuable IT resources and scale cost-effectively.

For more information, see the [BIG-IP Access Policy Manager](https://f5.com/products/modules/access-policy-manager) product page (f5.com/products/modules/access-policy-manager).

Sync using NTP with Remote Authentication Server

F5 recommends all BIG-IP systems have Network Time Protocol (NTP) configured for time consistency. Additionally, in BIG-IP APM, if the timestamp on an authentication request varies too far from the time on a remote authentication server, the request will likely be denied.

F5 recommends configuring BIG-IP APM to use the same NTP server(s) as any authentication servers that they will be communicating with to reduce the chances of users being denied due to time drift.

For more information about NTP, see [Networking and Cluster Health](#).

Configuration of Certificate for Access Virtual Server

As a security measure, F5 strongly recommends using a certificate from a trusted certification authority (CA) when providing client access in BIG-IP APM through a virtual server using a self-signed certificate.

Table 12.1: Recommended maintenance for BIG-IP APM

Task	Frequency
Check for OPSWAT updates	Monthly



BIG-IP Application Security Manager

BIG-IP Application Security Manager (ASM) is a flexible web application firewall that secures web applications in traditional, virtual, and private cloud environments. BIG-IP ASM provides unmatched web application and website protection, helps secure deployed applications against unknown vulnerabilities, and enables compliance for key regulatory mandates—all on a platform that consolidates application delivery with a data center firewall solution, and network and application access control.

For more information see the [BIG-IP Application Security Manager](https://f5.com/products/modules/application-security-manager) product page (f5.com/products/modules/application-security-manager).

F5 recommends checking for updates to the OPSWAT libraries on a monthly basis to ensure clients are only connecting with verified secure systems.

For more information, see [Software Updates](#), or see AskF5 article: [SOL10942: Installing OPSWAT hotfixes on BIG-IP APM systems](#).

Table 12.2: Recommended maintenance for BIG-IP ASM

Task	Frequency
Check for attack signature.	Monthly
Update license service check date.	Yearly
Test high availability configuration and fail over under controlled environment.	Every six months or before major application or configuration changes.
Review attack signature and policy settings.	Monthly or before major application changes.
Review policy violations on public networks.	Daily
Perform penetration testing.	Routinely

Update Attack Signatures

F5 recommends checking for new attack signature releases on a monthly basis to ensure you are always running the most up-to-date protection. This either can be a manual task, or scheduled automatically in the BIG-IP ASM configuration.

F5 releases a new attack signature update for BIG-IP ASM about every six weeks. These update include new attack signatures as well as enhancements to existing attack signatures. For more information, see [Software Updates](#), or see AskF5 article: [SOL8217: Updating the BIG-IP ASM attack signatures](#).

Update license service check date

F5 recommends updating the service check date for the BIG-IP APM module by reactivating the license on a yearly basis to ensure smooth installation of new attack signatures.

BIG-IP ASM attack signatures can only be updated on a BIG-IP system that has verified it has a valid support contract within the last 18 months.

For more information, see [Licenses and Entitlement](#), or see AskF5 article: [SOL8217: Updating the BIG-IP ASM attack](#)



[signatures.](#)

Test BIG-IP ASM sync and failover capabilities (high availability configurations only)

F5 recommends testing your high availability (HA) configuration and failing over under controlled conditions every six months or before major application or configuration changes to ensure application delivery will continue uninterrupted in the event of a real failure.

For more information, see Automatically Synchronizing Application Security Configurations in [BIG-IP Application Security Manager: Implementations](#) for your software version.

Review attack signature and policy settings

F5 recommends routine evaluation of application security needs and policies on a monthly basis or before major application changes to prevent unwanted behaviors from policies that no longer match their applications.

Applications grow and change as the needs of your business and customers do. A policy that was created for an application's release may no longer meet the security needs of that application as new features are added, or may contain orphaned configuration for application features that have changed or been removed. BIG-IP ASM Administrators work with Application Developers to evaluate routinely the security needs of the application; and how the policies are meeting those needs.

Review logged violations for accuracy

F5 recommends review of policy violations on a public network on a daily basis to gain insight into ongoing attacks or simple misconfigurations that may cause erroneously blocked traffic or log violations.

For a properly configured security policy on a public network, it's not uncommon for BIG-IP ASM to block traffic and log violations.

For more information, see [Log Files and Alerts](#), or Working with Violations in [BIG-IP Application Security Manager: Implementations for your software version](#).

Perform regular penetration testing

F5 recommends penetration testing against your security policies on a routine basis to ensure that your application is secure against malicious attackers.

Because of the variability of applications, environments, and security needs, F5 cannot recommend a specific period, but implementing a routine testing plan as part of your regular operations can help you identify and correct gaps in your Security Policy before an attacker does.

Remote logging for violations

F5 recommends setting up remote logging to provide historical archiving of violation data and to ensure that no important data is lost due to the limited violation storage constraints of BIG-IP ASM.



For more information, see [Log Files and Alerts](#) or Configuring Application Security Event Logging in [BIG-IP Application Security Manager: Implementations](#) for your software version.

Set up Simple Network Monitoring Protocol traps for violations

F5 recommends setting up Simple Network Monitoring Protocol (SNMP) traps to alert on you to attacks in progress. For more information, see the Log Files and Alerts chapter in this guide, or AskF5 article: [SOL7738: Configuring the BIG-IP ASM to send SNMP traps to communicate a blocked request and request violation](#).

Turn off learning for policies in blocking mode

F5 recommends turning off learning policies in blocking mode because these policies consume resources that can be better devoted to processing and securing traffic.

When set to blocking mode, a security policy is intended to protect your application, not learn about it. Freeing up resources spent on learning will help better and more efficiently protect your system.

For more information, see Refining Security Policies with Learning and Configuring Security Policy Blocking in [BIG-IP Application Security Manager: Implementations](#) for your software version.

Protect against application distributed denial-of-service (DDoS) attacks with BIG-IP ASM

Today's security threats increasingly involve application-layer distributed denial-of-service DDoS attacks mounted by organized groups of attackers to damage web-facing applications by exhausting resources. BIG-IP ASM provides application-layer protection against DDoS attacks.

BIG-IP ASM resides between applications and users and can detect and protect against an attack in real-time by:

- Detect an application is under attack.
- Identify attacker information.
- Mitigate the attack.

By controlling access, implementing challenge/response and anomaly detection engines, and applying the ability to understand application behavior, BIG-IP ASM defends against malicious connections and keeps attackers from overwhelming applications.

Detect an application attack

Recent application-level DDoS incidents show that such an attack can be described as a mass of HTTP requests to the web application from as many sources as possible.

Before DDoS was the common, the standard, single-point denial-of-service (DoS) attack prevailed. DoS attack uses a single source that sends as many requests as possible to affect application availability. A DDoS attack is mounted from multiple, geographically distributed locations as it tries to bypass traditional protection methods.



A security filter can easily detect an abnormal rate of HTTP requests sent from one source, as happens in a traditional DoS attack. Once detected, the attack can be mitigated easily by blocking access from the single source. DDoS is much more complex since it includes a multi-source attack with each source sending many HTTP requests. These attacks are usually conducted by ranks of ‘zombie’ PCs: devices infected by malware and controlled remotely by an anonymous attacker, often without the machine owners having any knowledge that an attack is underway.

To detect DDoS attacks, protection policies need to study how the attacked application is legitimately used, which can only be done by learning how the application is accessed over time, including all the characteristics of valid traffic. These characteristics typically include the following:

- Access rate over time. This identifies access rate to the application during different hours and days of the week. For example, some applications may draw Monday morning rush-hour traffic levels significantly differently from their traffic at other hours and on other days of the week.
- Rate per application resource. An application is not one organism but a collection of resources and each resource has its own characteristics. For example, there is no doubt that the access rate for an application login page is greater than for other pages in the application.
- Response latency. Application response latency for each application resource (and for the entire application) indicates when a resource is being exhausted.
- Rate of application responses. The rate of application responses such as 404 (page not found errors) and 500 (application errors) will change according to how the application is used.
- Geographical locations. User access rate can be segregated according to the users’ geographical location, and in many cases, web application administrators can predict their users’ location(s). For example, United States government web application administrators might anticipate that most users for most applications will be accessing those applications from within the U.S.

The detection of these traffic characteristics should be based on changes in the application behavior. For example, if the access rate of an application’s search page is typically 500 transactions per second and suddenly that rate jumps to 5000 transactions per second, it is usually safe to assume that the search page is being abused and possibly attacked. Depending on the source locations of each of those requests, the application may be subject to DDoS attack. In this example, the security filter should monitor the resource under attack rather than the source of the attack itself.

BIG-IP ASM detects such attacks by learning how the application is normally accessed. Depending on configuration, BIG-IP ASM generally accomplishes this by collecting the following information:

- Transactions per second for each URL in the application.
- Web server latency for each URL in the application.
- Transactions per second for each source IP that accesses the application.



BIG-IP ASM will detect an attack when there is a change in the way an application is being accessed compared to the normative values it has already learned.

Identify attacker information

After detecting that an application is under DDoS attack, the next step in defense is to determine who is attacking the application—or at least, what information can be discovered about the attacker(s). The challenge is to differentiate between the legitimate traffic and the attackers. By definition, a DDoS attack is mounted by many sources, so in the example of sudden jump to a high number of unusual search page requests, there will likely be multiple users trying to do valid searches on the application while others are participants in the attack.

The best way to differentiate legitimate from illegitimate traffic is to challenge users by distinguishing between normal users who work with browsers and malicious automatic tools that send requests directly to the application. One example for such a challenge is the CAPTCHA authentication test, which is used on many application login pages and attempts to repel brute-force attacks by requiring the user to respond to a random or personal challenge.

Another example of an effective challenge, and one used by BIG-IP ASM, is the injection of JavaScript to the user. Only clients who use a browser will pass this challenge, while malicious automated tools will fail it. As a result, BIG-IP ASM can selectively pinpoint and block those automated tools.

Detection and attacker identification are not always decisive. The complexity of the scenario affects the accuracy of detection efforts, and challenging detection tasks may result in false positives. In addition, failure to respond to a security challenge does not necessarily indicate an attack. For example, a challenge can fail to receive a response because of the users' browser limitations or configurations. Nevertheless, security measures with the ability to discern information about potential attackers and pose one or more challenges to suspicious users can more effectively detect and thus mitigate threats.

Mitigate an attack

As noted, application delivery is often a primary business goal and may be an organization's dominant—or only—customer interaction. In such cases, dropping application users' transactions is unacceptable, even when suspicious users fail to respond to a security challenge. Instead, efforts should be made to protect the application from DDoS attacks without denying legitimate traffic.

During a potential attack, several mitigation options are available:

- Delay access from suspicious source IPs.
- Delay access to URLs that are under attack.
- Drop connections for suspicious source IPs.
- Drop connections for URLs that are under attack.



Protect the application

If an attack occurs, it is important to mitigate the attack's effects on the application while preserving availability to legitimate traffic. One approach is to increase overall availability of an attacked resource by lowering the application access rate from suspicious sources. This has the effect of maintaining application quality of service while reducing service availability for suspicious users based on total available resources for the application. This approach has the added advantage of making it less likely that attackers will recognize that the attack is being mitigated. Using this approach, the application is protected while the worst case scenario for the legitimate user is that traffic slows.

BIG-IP Application Accelerator Manager

BIG-IP Application Acceleration Manager (AAM) combines the application delivery features previously available in BIG-IP WAN Optimization Manager™ (WOM®) and BIG-IP WebAccelerator.

You may run BIG-IP AAM on hardware appliances or VIPRION modular chassis and blade systems designed specifically for application delivery, or you may run BIG-IP AAM Virtual Edition (VE) on your choice of hypervisor and hardware.

For more information see the [BIG-IP Application Acceleration Manager](https://f5.com/products/modules/application-acceleration-manager) product page (f5.com/products/modules/application-acceleration-manager).

Increase data storage for BIG-IP AAM

You can use disk management to allocate dedicated disk space for the datastor service, which increases the data storage that BIG-IP AAM uses. Additional disk space is available in the following deployments.

Selected higher-end BIG-IP AAM platforms support the use of solid-state drives (SSDs) that come in a dual-disk drive sled and are installed along with hard disk drives.

If you are installing BIG-IP AAM Virtual Edition, you can select an extra disk deployment configuration. Systems with more than one drive or array may not come configured to use the additional storage.

Provision solid-state drives for datastor

datastor is the data storage used for optimization. By default, it is provisioned on the primary hard disk drive (HDD). To use solid-state drives (SSDs) on BIG-IP AAM, you must manually allocate the disk space on each SSD to the datastor service.



Important A BIG-IP AAM license is required to provision drives for datastor.

If you install SSDs after you have provisioned BIG-IP AAM, you must first disable BIG-IP AAM, then delete the datastor application volume from the primary disk before you assign the datastor service to the SSD volume. You then will have to re-enable BIG-IP AAM.

BIG-IP Policy Enforcement Manager

BIG-IP Policy Enforcement Manager (PEM) delivers the insight you need to understand subscriber behavior and effectively manage network traffic with a wide range of policy enforcement capabilities. BIG-IP PEM provides intelligent layer 4–7 traffic steering, network intelligence, and dynamic control of network resources through subscriber- and context-aware solutions. It also provides deep reporting, which you can capitalize on to build tailored services and packages based on subscribers' app usage and traffic classification and patterns to increase average revenue per user (ARPU).



Note IPFIX is a generic logging capability used by CGNAT, BIG-IP AFM, and PEM. If your IP Flow Information Export (IPFIX) collector is capable of TLS, F5 recommends specifying one of these terms of transport as the preferred transport when security is an issue.

For more information, see the [Policy Enforcement Manager](https://f5.com/products/service-provider-products/policy-enforcement-manager) product page (f5.com/products/service-provider-products/policy-enforcement-manager).

Enterprise Manager

Enterprise Manager significantly reduces the cost and complexity of managing multiple F5 devices. You gain a single-pane view of your entire application delivery infrastructure and the tools you need to automate common tasks, ensure optimized application performance, and improve budgeting and forecasting to meet changing business needs.

For more information, see the [Enterprise Manager](https://f5.com/products/modules/enterprise-manager) product page (f5.com/products/modules/enterprise-manager).

BIG-IP Link Controller

BIG-IP Link Controller puts the management of ISP links under your control. It monitors the performance and availability of each link and directs connections—both inbound and outbound—over the best possible link. It also improves application performance by prioritizing and optimizing traffic. BIG-IP Link Controller gives you the tools to direct traffic over the most cost-effective connections first so you can keep your ISP costs at a minimum.

For more information, see the [BIG-IP Link Controller product page](https://f5.com/products/modules/link-controller) (f5.com/products/modules/link-controller).

Carrier-Grade NAT

Carrier-Grade NAT (CGNAT) offers a broad set of tools that Service Providers (SPs) can use to migrate successfully to IPv6 while continuing to support and inter-operate with existing IPv4 devices and content. BIG-IP CGNAT offers SPs tunneling solutions such as Dual-Stack Lite and MAP along with native network address translation solutions such as NAT44 and NAT64. Carrier-grade scalability and performance is achieved by supporting a large number of IP address translations, very fast NAT translation setup rates, high throughput and flexible logging for subscriber traceability.



F5 recommends that you not deploy CGNAT with only a small address translation pool. The SP-DAG constraints of a source IP hash could result in some TMMs prematurely exhausting their quota of addresses and having to solicit help from a different TMM, which impairs performance. Generally, you need three times the number of translation addresses as TMMs to have a 90 percent chance of each TMM owning at least one address.

It is not advisable to enable CGNAT inbound connections unless absolutely necessary. The additional mapping constraints it imposes means more Public IP addresses are consumed. An external listener must also be created for each entry in the session database to check whether each inbound connection conforms.

To ensure service continuity when deploying deterministic NAT (DNAT) it is advisable to configure a backup (NAPT) source translation pool.

Avoid small block sizes when deploying CGNAT Port Block Allocation. If the size is set lower than the default of 64 you could jeopardize performance because the maximum connection rate and maximum number of concurrent connections will suffer.

Although the BIG-IP system supports a wide range of CGNAT logging options, for performance considerations you should only enable options you really need.



Note With the introduction of an off-box version of dnattutil, customers who want to use deterministic NAT (DNAT) mode must keep this version of the tool current since it can only interpret logs generated up to its current release. The latest version of the tool can be obtained from [F5 Downloads](https://downloads.f5.com) page (downloads.f5.com).

IPFIX is a generic logging capability used by CGNAT, BIG-IP AFM, and PEM. If your IP Flow Information Export (IPFIX) collector is capable of TLS, F5 recommends specifying one of these terms of transport as the preferred transport when security is an issue.

For more information, see the [Carrier-Grade NAT](https://f5.com/products/service-provider-products/carrier-grade-nat) product page (f5.com/products/service-provider-products/carrier-grade-nat).

View valid and expired licenses

For information about license status for your purchased modules, see the Licenses and Entitlement chapter in this guide.



Procedures

To disable BIG-IP AAM using the Configuration utility

1. Go to **System > Resource Provisioning**.
2. Find the Acceleration Manager (AM) list and note its current setting.
3. Select **None (Disabled)**.
4. Click **Submit**.
5. Click **OK**.

The BIG-IP system restarts without BIG-IP AAM provisioned.

6. Click **Continue**.

To delete datastor application volume using the Configuration utility

1. Go to **System > Disk Management**.

datastor allocation appears on one of the hard drives (for example **HD1**).
If it doesn't, you can skip the rest of this procedure.

2. Click the disk label for the drive containing the datastor allocation.
3. Under **Contained Software Volumes**, select **Datastor**.
4. Click **Delete**.

To provision SSDs for datastor using the Configuration utility

1. Go to **System > Disk Management**.
2. Click the SSD disk label (for example, **SSD1**).

The **General Properties** page opens for the logical disk you selected.

3. Under **General Properties**, for **Mode**, select **Datastor**.
4. Click **Update**.
5. Repeat for each SSD displayed on the **System > Disk Management** page.

To re-enable BIG-IP AAM using the Configuration utility

1. Go to **System > Resource Provisioning**.



2. From the **Acceleration Manager (AM)** list, select **Nominal** (or its previous setting, which you noted when you disabled it).
3. Click **Update**.
4. Click **OK**.

The BIG-IP system restarts with BIG-IP AAM provisioned. This may take a minute or so.

5. Click **Continue**.

The datastor service is now allocated to the SSDs. The datastor volume spans the installed SSDs. You can verify the result by checking the **Disk management page**. The logical view displays the datastor allocation for each disk.

Monitor SSD use

If you are using solid-state drives (SSDs) for datastor, you can view the SSD allocation and monitor the SSD lifespan.

To monitor the SSD lifespan using the Configuration utility

1. Go to **System > Disk Management**.
2. Click the disk label for the disk you want to monitor.
3. Note which bays contain SSDs.
4. View the **Media Wearout Indicator** to monitor disk usage.



Additional resources

The following table points to additional resources you can visit to learn more about the concepts and areas mentioned in this chapter. You can find AskF5 solution articles and the right product manuals for your software version by searching [AskF5 \(support.f5.com\)](https://support.f5.com).

Table 12.3: Additional resources

For more information about	See
BIG-IP Protocol Security Module (PSM).	AskF5 BIG-IP PSM product page (support.f5.com/kb/en-us/products/big-ipm.psm.html).
BIG-IP DNS.	AskF5 BIG-IP DNS/GTM product page (support.f5.com/kb/en-us/products/big-ip_gtm.html).
BIG-IP Local Traffic Manager (LTM).	AskF5 BIG-IP LTM product page (support.f5.com/kb/en-us/products/big-ip_ltm.html).
BIG-IP Advanced Firewall Manager (BIG-IP AFM).	AskF5 BIG-IP AFM datasheet (https://www.f5.com/pdf/products/big-ip-advanced-firewall-manager-datasheet.pdf).
BIG-IP Access Policy Manager (APM).	AskF5 BIG-IP APM product page (support.f5.com/kb/en-us/products/big-ip_apm.html).
BIG-IP Application Security Manager (ASM).	AskF5 ASM product page (support.f5.com/kb/en-us/products/big-ip_asm.html).
BIG-IP Application Acceleration Manager (AAM).	AskF5 AAM product page (support.f5.com/kb/en-us/products/big-ip-aam.html).
BIG-IP Policy Enforcement Manager (PEM).	AskF5 PEM product page (support.f5.com/kb/en-us/products/big-ip-pem.html).
Carrier-Grade NAT.	Carrier-Grade NAT product page (f5.com/products/service-provider-products/carrier-grade-nat).
BIG-IP Link Controller.	AskF5 BIG-IP Link Controller product page (support.f5.com/kb/en-us/products/lc_9_x.html).
Enterprise Manager (EM).	AskF5 Enterprise Manager product page (support.f5.com/kb/en-us/products/em.html).

Help improve this guide

Please help F5 improve this guide by responding to a few questions about this chapter.

(Note: You must be viewing this document in Adobe Acrobat Reader or similar to use this form.)

Did this chapter answer all of your questions about the subject matter? Yes No

If not, what information should be included that is not? _____

Did you find any errors pertaining to subject matter in this chapter? Yes No

If yes, please describe the error: _____

If yes, please copy and paste the paragraph containing the error here: _____

Did you find non-subject-matter errors in this chapter (spelling, etc.)? Yes No

If yes, please describe the error: _____

If yes, please copy and paste the paragraph containing the error here: _____



MySQL

Background

Important

- It is not necessary to do any optimization or maintenance tasks for a MySQL deployment.
- F5 does not support direct manipulation of the MySQL database.
- Do not do operations on the MySQL database unless directed to do so by F5 Support.
- Even for extremely busy BIG-IP systems, use of the MySQL database by the BIG-IP system is typically very light.

MySQL database daemon

Your BIG-IP system includes the MySQL database daemon. This daemon is always running and tracks the following:

- BIG-IP AFM (Advanced Firewall Manager) DoS/DDoS information and policy logs.
- BIG-IP ASM (Application Security Module) policies.
- AVR (Application Visibility and Reporting) statistics.
- BIG-IP APM (Access Policy Manager) request logging.

F5 has implemented the following measures by default:

- BIG-IP ASM policies are automatically exported and included in a UCS backup. For more information, see [Backup and Data Recovery](#).
- AVR statistics are regularly purged to keep the size of the tables under a million records, and the overall size of the database under 2GB.
- BIG-IP APM log data is regularly purged to keep the maximum number of entries under 5 million records.

Special requirements

If you have special requirements of the MySQL database, such as exporting of the data to long-term storage, it is best to contact [F5 Consulting](#) (f5.com/support/professional-services) for assistance in creating a supported solution.

Additional resources

The following table points to additional resources you can visit to learn more about the concepts and areas mentioned in this chapter. You can find AskF5 solution articles and the right product manuals for your software version by searching [AskF5](#) (support.f5.com).



Table 13.1: Additional resources

For more information about	See
Troubleshooting the BIG-IP ASM MySQL database	SOL14194: Troubleshooting the BIG-IP ASM MySQL database.



Caches

At a glance—Recommendations

F5 has identified the following cache recommendations:

- Let cache objects time out and expire without intervention.
- Manage and maintain the contents that are stored in cache.
- View cache utilization on a weekly basis if memory and disk utilization is higher than normal.
- Determine DNS cache performance and statistics.
- Invalidate cached content for an application and node when updating content every hour or every day.
- Manage BIG-IP AAM caching behavior by examining the X-WA-info debug headers and the BIG-IP AAM dashboard.

Background

This section provides context for our recommended procedures in the form of overviews and supplemental information.

BIG-IP cache feature

The BIG-IP Cache Setting feature, formerly known as RAM Cache, uses the information from the Vary header to cache responses from the origin web server (OWS). OWS can include information within the Vary header to determine which resource the server returns in its response.

For example, if a page is optimized for a particular web browser, OWS response may return the Vary: User-Agent HTTP header. The proxy server then uses this information to determine whether to return a cached copy of the response to subsequent requests, or to query the OWS for the resource again (a subsequent client request containing a different User-Agent value forces the proxy to query the OWS for the resource again).

An HTTP cache is a collection of HTTP objects stored in the BIG-IP system memory which subsequent connections can reuse to reduce traffic load on the origin web servers. The goal of caching is to reduce the need to send frequent requests for the same object, and eliminate the need to send full responses in many cases. You can enable HTTP caching on the BIG-IP system by associating a Web Acceleration profile with a virtual server.



Note Web Accelerator is not supported in v11.4 and later.



Cacheable content

The BIG-IP cache feature complies with the cache specifications described in RFC 2616. You can configure the BIG-IP system to cache the following content types:

- 200, 203, 206, 300, 301, and 410 HTTP responses.
- Responses to HTTP GET requests.
- Other HTTP methods for uniform resource identifiers (URIs) specified for inclusion in cached content, or specified in an iRule.
- Content based on the User-Agent and Accept-Encoding values. The cache feature holds different content for Vary headers.

The default cache configuration caches only responses to HTTP GET requests. However, you can configure the Web Acceleration profile to cache other requests, including non-HTTP requests. To do this, you can specify a URI in the URI Include or Pin List within an HTTP profile, or write an iRule.

Non-cacheable content

The cache feature does not cache the following items:

- Private data specified by cache control headers.
- Action-oriented HTTP methods such as HEAD, PUT, DELETE, TRACE, and CONNECT.
- Set-Cookie headers sent by the origin web server.

BIG-IP DNS cache feature

You can configure a transparent cache on the BIG-IP system to use external DNS resolvers to resolve queries and then cache the responses from the resolvers. The next time the system receives a query for a response that exists in the cache, the system immediately returns the response from the cache. The transparent cache contains messages and resource records.

A transparent cache in the BIG-IP system consolidates content that would otherwise be cached across multiple external resolvers. When a consolidated cache is in front of external resolvers (each with their own cache), it can produce a much higher cache hit percentage.

BIG-IP AAM optimization cache feature

BIG-IP AAM optimization cache is a self-managing feature. A small amount of TMM memory is used together with a disk-based datastore/metastore database. The two ways to view BIG-IP AAM caching behavior are by using X-WA-Info debug headers and through the dashboard in the Configuration utility.



Procedures

Display cache setting entries at the command line

You can display the contents of the Cache Setting feature with the command line using the `tmsh ramcache` command. The **ramcache** command includes a number of other options that you can use to display only those Cache Setting entries corresponding to specific uniform resource identifiers (URIs), URI branches, or hosts.

For more information about using `tmsh` to manipulate Cache Setting entries, see [Traffic Management Shell \(tmsh\) Reference Guide](#).

To display the Cache Setting entries for a particular profile at the command line

1. Log in to the Traffic Management Shell (`tmsh`) at the command line by typing the following command:

```
tmsh
```

2. At the command prompt, type:

```
show ltm profile ramcache <profilename>
```

All of the HTTP cache entries on the BIG-IP system will be displayed.

To display the Cache Setting entries on BIG-IP AAM at the command line

1. Log in to the Traffic Management Shell (`tmsh`) at the command line by typing the following command:

```
tmsh
```

2. At the command prompt, type:

```
show ltm profile web-acceleration <profilename>
```

To determine percentage of memory used by each TMM process at the command line

- At the command prompt, type:

```
tmctl -d blade tmm/pagemem
```

To view DNS cache statistics using `tmsh` at the command line

1. Log in to the Traffic Management Shell (`tmsh`) at the command line by typing the following command:

```
tmsh
```

2. At the command prompt, type:

```
show ltm dns cache
```

Statistics for all of the DNS caches on the BIG-IP system display.

3. At the command prompt, type:



```
show ltm dns cache <cache-type>
```

To display statistics for each transparent cache using tmsh at the command line

1. Log in to the Traffic Management Shell (tmsh) at the command line by typing the following command:

```
tmsh
```

2. At the command prompt, type syntax:

```
show ltm dns cache <cache type> <cache name>
```

Example:

```
show ltm dns cache transparent test
```

Statistics for the transparent cache on the system named test display.

To view DNS cache statistics using the Configuration utility

1. Go **Statistics > Module Statistics > Local Traffic**.
2. For **Statistics Type**, select **DNS Cache**.
3. Click **View**.

To view DNS cache records using tmsh at the command line

1. Log in to the Traffic Management Shell (tmsh) at the command line by typing the following command:

```
tmsh
```

2. At the command prompt, type syntax:

```
show ltm dns cache <cache type> <cache name>
```

Example:

```
show ltm dns cache transparent test
```

Manage transparent cache size

To determine the amount of memory a BIG-IP system has installed and how much of that memory to commit to DNS caching, you can view the statistics for a cache to determine how well the cache is working. You can also change the size of a DNS cache to fix cache performance issues.

To modify cache statistics using the Configuration utility

1. Go to **DNS > Caches > Cache List**.
2. Click the name of the cache you want to modify.



3. In **Message Cache Size**, type the maximum size in bytes for the DNS message cache.

The BIG-IP system caches the messages in a DNS response in the message cache. A larger maximum size makes it possible for more DNS responses to be cached and increases the cache hit percentage. A smaller maximum size forces earlier eviction of cached content, but can reduce the cache hit percentage.

4. In **Resource Record Cache Size**, type the maximum size in bytes for the DNS resource record cache.

The BIG-IP system caches the supporting records in a DNS response in the Resource Record cache. A larger maximum size makes it possible for more DNS responses to be cached and increases the cache-hit percentage. A smaller maximum size forces earlier eviction of cached content, but can reduce the cache hit percentage.



Note The message caches size include all TMMs on the BIG-IP system. If there are eight TMMs, multiply the size by eight and put that value in this field.

Invalidate cached content

Cache invalidation is a powerful tool that you can use to maintain tight coherence between the content on your origin web servers and the content that the BIG-IP system caches.

If you update content for your site at regular intervals, such as every day or every hour, you can use lifetime rules to ensure that the system's cache is refreshed with the same frequency.

Invalidation rules allow you to “expire” cached content before it has reached its time to live (TTL) value. Invalidation rules are good to use when content updates are event-driven, such as when an item is added to a shopping cart, a request contains a new auction bid, or a poster has submitted content on a forum thread.



Note Invalidating the cached content on the BIG-IP system temporarily increases traffic to the origin web servers until the BIG-IP module repopulates the cache.



To invalidate cache content using the Configuration utility

1. Go to **Acceleration > Web Application > Invalidate Content**.
2. For the application cache you want to invalidate, select the check box.
3. Click **Invalidate**.

Enable X-WA-Info headers for testing or troubleshooting

WA-Info HTTP headers are headers that are optionally inserted into responses to the client by the BIG-IP AAM system to provide information on how the response was processed. This facility and the Dashboard provide the only facilities to track the behavior of BIG-IP AAM web optimization cache.



Note The X-WA-Info headers feature should only be active in testing or troubleshooting and usually will be requested by F5 Support. It should not be left on in a production environment as there is an associated processing overhead providing this information in every transaction in the network traffic.

To enable X-WA-Info headers using the Configuration utility

1. Go to **Acceleration > Web Applications > Applications**.
2. Choose the appropriate application, then go to **Advanced**.
3. Go to **Debug Options**.
4. For **X-WA-Info Header** option, select **Standard** or **Debug**.

BIG-IP AAM dashboard utility

The dashboard default reporting page summarize information about the memory, performance, throughput, and cache behavior of BIG-IP AAM. These include the following:

- Web Optimized.
- Transactions Web Image.
- Optimization Optimized.
- Web Throughput Web.
- Cache Effectiveness.

- Web Cache Invalidations.
- Memory Usage.

Web optimized transactions

This page displays performance metrics for cached transactions in tabbed views, including **From cache**, **Proxied**, and **Errors**. A combined view is also available.

From cache shows cached transactions per second against time, collected in increments of **5 minutes**, **3 hours**, **24 hours**, **1 week**, or **1 month**. You can point to the line in the graph to display a specific time and number of cached transactions per second. If configuration changes were made, a red circle appears in the graph, which you can click to view additional details.

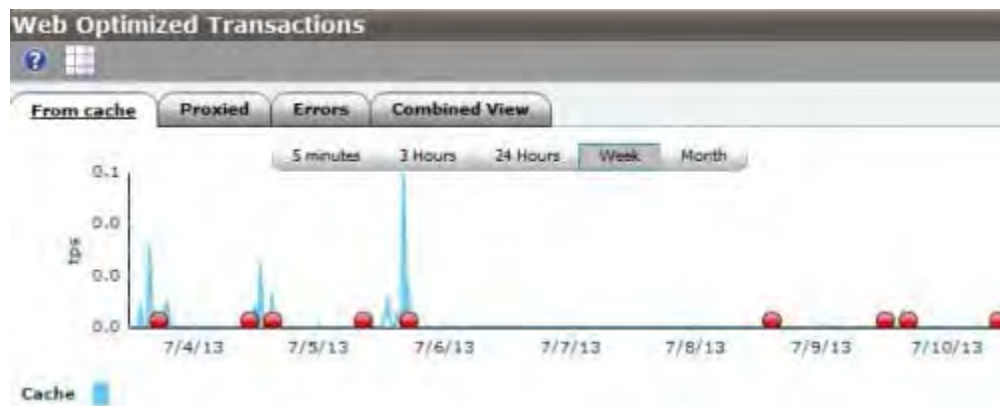


Figure 14.1 Web Optimized Transaction page, From cache view

Optimized Web Throughput

This page displays selectable throughput metrics in tabbed views, including From cache and Proxied. A combined view is also available.

From cache shows cached bytes per second against time, collected in increments of **5 minutes**, **3 hours**, **24 hours**, **1 week**, or **1 month**. You can point to the line in the graph to display a specific time and number of cached bytes per second. If configuration changes were made, a red circle appears in the graph, which you can click to view additional details.



Figure: 14.2 Optimized Web Throughput page, From cache view

Web Cache Effectiveness

This page displays selectable cache metrics in tabbed view, including **Entries**, **Bytes**, and **Evictions**. A combined view is also available.

- Entries shows the number of cached entries against time, collected in increments of **5 Minutes**, **3 Hours**, **24 Hours**, **1 Week**, or **1 Month**. You can point to the line in the graph to display a specific time and number of cached entries. If configuration changes were made, a red circle appears in the graph, which you can click to view additional details.
- Bytes shows the total size of cached entries (in bytes) against time, collected in increments of **5 Minutes**, **3 Hours**, **24 Hours**, **1 Week**, or **1 Month**. You can point to the line in the graph to display a specific time and total size of entries in bytes. If configuration changes were made, a red circle appears in the graph, which you can click to view additional details.
- Evictions shows the number of cached evictions against time, collected in increments of **5 Minutes**, **3 Hours**, **24 Hours**, **1 Week**, or **1 Month**. You can point to the line in the graph to display a specific time and number of evictions. If configuration changes were made, a red circle appears in the graph, which you can click to view additional details.

Web Image Optimization

This page displays selectable image metrics in tabbed view, including **Current Reduced**, **Total Reduced**, **Current Savings**, **Total Saving**, **Average Size**, and **Images Optimized**. A combined view is also available.



Figure: 14.3 Web Image Optimization page, Current Reduced view

Web Cache Invalidations

This page displays selectable invalidations metrics in a tabbed view, including Triggered Sourced, Triggered Received, ESI Sourced, and ESI Received. A combined view is also available.

To easily check for an Invalidation trigger, set the time period to **3 Hours** and watch the far right of the page for a small peak to appear. Wait a few moments, then switch the time period to **5 Minutes**. The page takes time collecting and adjusting the display of the data over the entire page time axis.

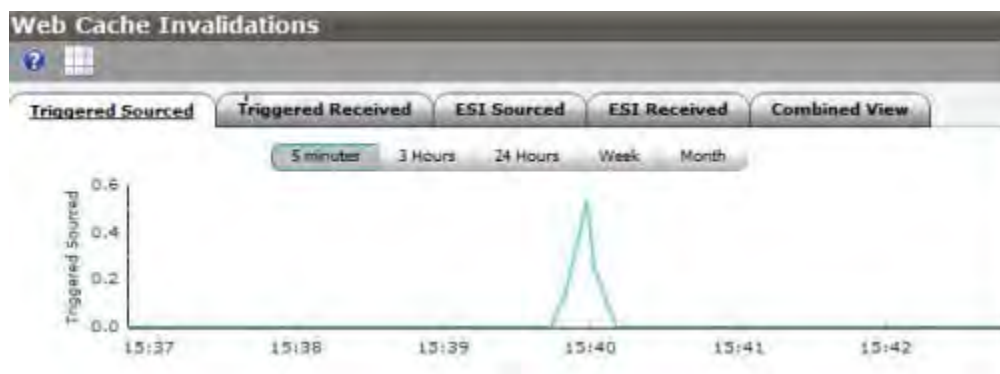


Figure: 14.4 Web Cache Invalidations page, Triggered Sourced view



Additional resources

The following table points to additional resources you can visit to learn more about the concepts and areas mentioned in this chapter. You can find AskF5 solution articles and the right product manuals for your software version by searching [AskF5 \(support.f5.com\)](https://support.f5.com).

Table 14.5: Additional resources

For more information about	See
Overview of the Web Acceleration profile.	SOL14903: Overview of the Web Acceleration profile.
Displaying cache setting entries via CLI.	SOL13255: Displaying and deleting Cache Setting entries from the command line (11.x).
DNS Caches.	DNS Cache: Implementations in the BIG-IP LTM Guide.
SNMP MIB files.	SOL13322: Overview of BIG-IP MIB files (10.x - 11.x).
Memory allocation for the BIG-IP Cache Setting feature.	SOL13878: The 'ramcache.maxmemorypercent' variable controls memory allocation for the BIG-IP Cache Setting feature (11.x).
HTTP Vary header functionality.	SOL5157: BIG-IP LTM Cache Setting feature and HTTP Vary header functionality.

Help improve this guide

Please help F5 improve this guide by responding to a few questions about this chapter.

(Note: You must be viewing this document in Adobe Acrobat Reader or similar to use this form.)

Did this chapter answer all of your questions about the subject matter? Yes No

If not, what information should be included that is not? _____

Did you find any errors pertaining to subject matter in this chapter? Yes No

If yes, please describe the error: _____

If yes, please copy and paste the paragraph containing the error here: _____

Did you find non-subject-matter errors in this chapter (spelling, etc.)? Yes No

If yes, please describe the error: _____

If yes, please copy and paste the paragraph containing the error here: _____



External APIs

At a glance—Recommendations

F5 has not identified any recommendations for this section.

Background

This section provides context for our recommended procedures in the form of overviews and supplemental information.

BIG-IP APIs and automation interfaces

The BIG-IP system has a number of external APIs and interfaces, which are useful for a wide range of administrative functions, including configuration, monitoring, and reporting. These APIs and interfaces do not need to be maintained.

The BIG-IP system contains or uses the following APIs and programming/automation interfaces:

- Traffic Management Shell (tmsh).
- iControl.
- iApps®.
- iCall®.
- iRules.
- iControl® REST.
- iControl® SOAP.
- SNMP (Simple Network Management Protocol).

Traffic Management Shell (tmsh)

The Traffic Management Shell (tmsh) is the BIG-IP command-line interface (CLI). It shares many of the same properties and features of other networking and systems industry shells, such as GNU Bourne Again Shell (BASH), Cisco IOS, and Juniper JunOS. tmsh uses a Tool Command Language (Tcl) syntax and command-set, which has been expanded and extended by F5 for tmsh.

- BIG-IP single configuration file (SCF) and on-disk configuration files are all written in native tmsh syntax and have advanced scripting capabilities, all based on F5 enhancements to Tcl.
- tmsh is the basis for other interfaces, such as iApps and iCall, and is the base mapping for iControl REST. (See [iControl](#), [iApps](#), and [iCall](#).)
- tmsh can be used to automate any tmsh commands.



Example:

```
tmsh help /cli script
```

- `tmsh` contains a built-in help system.

Files related to `tmsh`

- **`/config/bigip_script.conf`** — Stores `tmsh` scripts added to the system.
- **`/config/bigip_user.conf`** — User configuration, including shell preference.
- **`/config/bigip_base.conf`** — Management interface configuration.
- **`/config/bigip.conf`** — Self-IP configuration.

Logs related to `tmsh`

- **`/var/log/ltm`** — Default location for most core BIG-IP messages.
- **`/var/log/audit.log`** — Audit logging, if auditing is enabled.

iControl

iControl is the open, web services-based API used by the BIG-IP system that allows complete, dynamic, programmatic control of F5 configuration objects. It enables applications to work in concert with the underlying network based on true software integration.

iControl comes in two forms, iControl SOAP and its successor iControl REST. While both forms are supported, iControl SOAP is no longer being fully developed and is in the process of being deprecated. New implementations should use iControl REST.

iControl SOAP is based on Simple Object Access Protocol (SOAP), a legacy protocol which was once very popular for web-based APIs. iControl SOAP was released in BIG-IP version 9.0. It is more difficult to program in than iControl REST, but external libraries are available to assist in writing code.

iControl REST uses modern web standards in the form of Representational State Transfer (REST) and JavaScript Object Notation (JSON). iControl REST is used in BIG-IP systems 11.4 and later. Its API is based on `tmsh`, sharing the same overall layout and structure. It is essentially a JSON version of `tmsh` that adheres to REST standards. iControl REST complies with modern web-based programming paradigms and is easier to use and implement than iControl SOAP.

iControl automation is generally written using systems and languages external to the BIG-IP system. It is the responsibility of the customer to ensure they are properly versioned and backed up.

Logs related to iControl

- **`/var/log/ltm`** — Default location for most core BIG-IP messages.
- **`/var/log/audit.log`** — Audit logging, if auditing is enabled.



iApps

iApps is the BIG-IP system framework for deploying services-based, template-driven configurations on BIG-IP systems running TMOS 11.0.0 and later. iApps allows creation of application-centric deployment interfaces on BIG-IP systems, reducing configuration time and increasing accuracy of complex traffic management implementations. The goal of iApps is to enable Subject-Matter Experts (SME) to build finely tuned configurations that can be deployed by administrators who possess application-level expertise without requiring them to be concerned about lower-level networking details.

The iApps is primarily used to package and deliver expert-created configurations to a non-expert audience. Its implementation language is standard tmsh scripting with environmental variables for Application Presentation Language (APL) user selections. It uses the F5-specific APL to render a user-facing presentation interface. It allows prescriptive abstraction of repeatable configurations based on user-facing input.

Configuration information is stored in UCS/SCF backups by default, with no special action required. For more information, see [Backup and Data Recovery](#).

Files related to iApps

- **/config/bigip_script.conf** — Stores iApp Templates added to the system.

Logs related to iApps

- **/var/tmp/script.log** — All non-APL output from iApp Templates goes to this file.

iCall

iCall is an event-based automation system for the BIG-IP control plane, introduced in BIG-IP v. 11.4. It can send and receive external events using any ports or protocols and can be useful for integration into upstream orchestration, or for driving orchestration directly from the BIG-IP system.

It uses standard tmsh syntax and is still in the early phases of development, so there is minimal documentation. All events are user-defined and none of the internal events are currently exposed.

Configuration information is stored in UCS/SCF backups by default, with no special action required. For more information, see the Backup and Data Recovery chapter in this guide.

Files related to iCall

- **/config/bigip_script.conf** — Stores all iCall configuration and scripts added to the system.

Logs related to iCall

- **/var/tmp/script.log** — All output from iCall scripts goes to this file.



iRules

iRules is a powerful and flexible feature within BIG-IP Local Traffic Manager that you can use to manage your network traffic. Using syntax based on the industry-standard Tools Command Language (Tcl), greatly enhanced by F5, iRules not only allows you to select pools based on header data, but also allows you to direct traffic by searching on any type of content data that you define. Thus, the iRules feature significantly enhances your ability to customize your content switching to suit your exact needs.

iRules fully exposes BIG-IP internal Traffic Management Microkernel (TMM) packet/data processing, allowing inspection, manipulation and optimization and contains a number of mechanisms for exporting information out of the data-plane.

Out-of-band/side-band connections: Enable asynchronous communication with outside hosts from within TMM/iRules. (For more information, see [iRules Sideband documentation](#) on [DevCentral](#) (devcentral.f5.com/wiki/iRules.SIDEBAND.ashx).

Important iRules terms

- **iFiles:** Stores data/content files and external class-lists for use by iRules.
- **iStats:** iRules variables that are accessible in tmsh and the other control-plane languages (iApps, iCall, and so on.). It is the primary vehicle for information sharing between control-plane and data-plane.

iRules management

Configuration information is stored in UCS/SCF backups by default, with no special action required. For more information, see the Backup and Data Recovery chapter in this guide.

Files related to iRules

- **/config/bigip.conf** — Stores all iRules added to the system.

Logs related to iRules

- **/var/log/ltm** — All logging output from iRules goes to this file.

Simple Network Management Protocol (SNMP)

SNMP is an industry-standard application-layer protocol, most commonly used by centralized monitoring and automation systems. It is a part of the TCP/IP protocol suite.

SNMP Management

Configuration information is stored in UCS/SCF backups by default, with no special action required. For more information, see the Backup and Data Recovery chapter in this guide.

The supported method for modifying the SNMP configuration is using tmsh. Editing the SNMP configuration files directly is not supported and will likely result in loss of configuration changes.



Files related to SNMP

- **/config/bigip_base.conf** — Stores SNMP configuration, as configured using tmsh.

Logs related to SNMP

- **/var/log/snmpd.log** — All logging output from SNMP goes to this file.

Procedures

There are no specific procedures required for maintaining the operational efficiency of these interfaces. However, there are some recommended practices to keep in mind when implementing them.

Recommended practices

The BIG-IP system APIs and interfaces are powerful tools and must be created and maintained with the same care as any other software development project. Inconsistent naming conventions, missing code comments, and unreviewed code combined with weak change management is the source of many upgrade and maintenance issues.

Coding best practices with BIG-IP APIs

- Use Port Lockdown to limit access to necessary interfaces/ports.
- Always develop and test in a non-production environment (BIG-IP VE, for example).
- Use consistent syntax and style.
- Be sure to comment effectively and implement revision control.
- Audit all BIG-IQ® system automation and scripting prior to upgrade to determine ongoing support for the APIs and interfaces employed.

For more information, see [Appendix B: Deployment and Response Methodologies](#).

Upgrades

- Before upgrading, verify there are no behavior changes when upgrading in a lab or pre-production environment.
- After upgrading, confirm operation and functionality of each interface.

For more information, see [Appendix B: Deployment and Response Methodologies](#).

Log review

Logs should be regularly reviewed for alerts or errors.

- All alert/error messages should be investigated and documented.



- Warnings should also be investigated to determine their relevance and any necessary actions.
- Debug logging should only be used during troubleshooting. This is especially true for iRules, which can influence production traffic negatively.
- Debug logging should be very specific to what is being investigated, due to verbose logging and high volume of messages.

For more information, see [Log Files and Alerts](#).

tmsh authentication and authorization configuration

Configuration information is stored in UCS/SCF backups by default, with no special action required. For more information, see [Backup and Data Recovery](#).

Each user can individually configure their tmsh default shell.

To configure a user's tmsh default shell at the command line

- At the command prompt, type the following command syntax:

```
tmsh: modify auth user [username] shell tmsh
```

To configure a user's tmsh default shell using the Configuration utility

1. Go to **System > Users > User List**.
2. Click the user name.
3. In **Terminal Access**, select **tmsh**.
4. Click **Update**.

Set up Self IP Port Lockdown to accept tmsh traffic on port 22

Port Lockdown specifies the protocols and services from which a self IP address can accept traffic. It is a security feature that allows you to specify particular UDP and TCP protocols and services from which the Self IP address can accept traffic. By default, a Self IP address accepts traffic from these protocols and services:

- For UDP, the allowed protocols and services are: DNS (53), SNMP (161), RIP (520).
- For TCP, the allowed protocols and services are: SSH (22), DNS (53), SNMP (161), HTTPS (443), 4353 (iQuery®).

tmsh uses Secure Shell (SSH) on port 22. MGMT: Port 22 is available on the management interface by default. To allow Self IP addresses to receive traffic for tmsh, you need to configure Port Lockdown.

**To configure self IP Port Lockdown at the command line**

- At the command prompt, type the following command syntax:

```
modify net self <ip address> allow-service add { tcp:22 }
```

To configure self IP Port Lockdown using the Configuration utility

1. Go to **Network > Self IPs**.
2. Click the IP address you want to configure.
3. In **Port Lockdown**, select the port and protocol that you want to allow.
4. Click **Finished**.

For more information, see Configuring Self IP Addresses in [TMOS Management Guide for BIG-IP Systems](#).

iControl authentication and authorization configuration

iControl uses the same user role as tmsh and the BIG-IP Configuration utility.

To assign iControl administrative rights to a user at the command line

1. Log in to the Traffic Management Shell (tmsh) by typing the following command:

```
tmsh
```

2. At the command prompt, type:

```
modify auth user <username> role admin
```

To assign iControl administrative rights to a user using the Configuration utility

1. Go to **System > Users > User List**.
2. Click the user name of the user you want to modify.
3. In the **Role** menu, click **Administrator**.
4. Click **Update**.

Self IP Port Lockdown

Set up Self IP Port Lockdown to limit access to necessary interfaces and ports

Port Lockdown specifies the protocols and services from which a self IP address can accept traffic. It is a security feature that allows you to specify particular UDP and TCP protocols and services from which the Self IP address can accept traffic. By default, a Self IP address accepts traffic from these protocols and services:



- For UDP, the allowed protocols and services are: DNS (53), SNMP (161), RIP (520)
- For TCP, the allowed protocols and services are: SSH (22), DNS (53), SNMP (161), HTTPS (443), 4353 (iQuery)



Note MGMT: Port 443 is available on the management interface by default. BIG-IP versions 11.6.0 and earlier do not support port filtering on the MGMT port interface.

To configure Self IP Port Lockdown at the command line

1. Log in to the Traffic Management Shell (tmsh) by typing the following command:

```
tmsh
```

2. At the command prompt, type syntax:

```
modify net self <ip address> allow-service add { tcp:443 }
```

To configure Self IP Port Lockdown using the Configuration utility

1. Go to **Network > Self IPs**.
2. Click the IP address you want to configure.
3. In **Port Lockdown**, select the port and protocol that you want to allow.
4. Click **Finished**.

For more information, see Configuring Self IP Addresses in [TMOS Management Guide for BIG-IP Systems](#).

iApps authentication and authorization configuration

To assign iApps administrative rights to a user at the command line

1. Log in to the Traffic Management Shell (tmsh) by typing the following command:

```
tmsh
```

2. At the command prompt, type:

```
modify auth user <username> role admin
```

To assign iApps administrative rights to a user using the Configuration utility

1. Go to **System > Users > User List**.
2. Click the user name of the user you want to modify.



3. In the **Role** menu, click **Administrator**.
4. Click **Update**.

Self IP Port Lockdown

Set up Self IP Port Lockdown to limit access to necessary interfaces and ports

Port Lockdown specifies the protocols and services from which a Self IP address can accept traffic. It is a security feature that allows you to specify particular UDP and TCP protocols and services from which the Self IP address can accept traffic. By default, a Self IP address accepts traffic from these protocols and services:

- For UDP, the allowed protocols and services are: DNS (53), SNMP (161), RIP (520).
- For TCP, the allowed protocols and services are: SSH (22), DNS (53), SNMP (161), HTTPS (443), 4353 (iQuery).



Note MGMT: Port 443 is available on the management interface by default. BIG-IP versions 11.6.0 and earlier do not support port filtering on the MGMT port interface.

1. Log in to the Traffic Management Shell (tmsh) by typing the following command:

```
tmsh
```

2. At the command prompt, type syntax:

```
modify net self <ip address> allow-service add { tcp:443 }
```

To configure Self IP Port Lockdown using the Configuration utility

1. Go to **Network > Self IPs**.
2. Click the IP address you want to configure.
3. In **Port Lockdown**, select the port and protocol that you want to allow.
4. Click **Finished**.

For more information, see Configuring Self IP Addresses in [TMOS Management Guide for BIG-IP Systems](#).

iCall authentication and authorization configuration

To assign iCall administrative rights to a user at the command line

1. Log in to the Traffic Management Shell (tmsh) by typing the following command:

```
tmsh
```

2. At the command prompt, type:



```
modify auth user <username> role admin
```

To assign iCall administrative rights to a user using the Configuration utility

1. Go to **System > Users > User List**.
2. Click the user name of the user you want to modify.
3. In the **Role** menu, click **Administrator**.
4. Click **Update**.

iCall access

iCall is a local event system for the BIG-IP system. It does not have any ports available.

Self IP Port Lockdown

Set up Self IP Port Lockdown to limit access to necessary interfaces and ports

Port Lockdown specifies the protocols and services from which a self IP address can accept traffic. It is a security feature that allows you to specify particular UDP and TCP protocols and services from which the self IP address can accept traffic. By default, a self IP address accepts traffic from these protocols and services:

- For UDP, the allowed protocols and services are: DNS (53), SNMP (161), RIP (520)
- For TCP, the allowed protocols and services are: SSH (22), DNS (53), SNMP (161), HTTPS (443), 4353 (iQuery)tmsh uses SNMP on ports 161 and 162 (traps).



Note MGMT: Ports 161 and 162 are available on the management interface by default. BIG-IP versions 11.6.0 and earlier do not support port filtering on the MGMT port interface.

**To configure Self IP Port Lockdown at the command line**

1. Log in to the Traffic Management Shell (tmsh) by typing the following command:

```
tmsh
```

2. At the command prompt, type syntax:

```
modify net self <ip address> allow-service add { tcp:161 tcp:162 }
```

To configure self IP Port Lockdown using the Configuration utility

1. Go to **Network > Self IPs**.
2. Click the IP address you want to configure.
3. In **Port Lockdown**, select the port and protocol that you want to allow.
4. Click **Finished**.

For more information, see Configuring Self IP Addresses in [TMOS Management Guide for BIG-IP Systems](#).

SNMP authentication and authorization configuration**To configure SNMP at the command line**

1. Log in to the Traffic Management Shell (tmsh) by typing the following command:

```
tmsh
```

2. At the command prompt, type:

```
tmsh help /sys snmp
```

SNMP automation is written using systems and languages external to the BIG-IP system. It is the responsibility of the customer to ensure they are properly versioned and backed up.



Important There is no user-based authentication or authorization for SNMP. Anyone with access to the port can send and receive information. Do not expose SNMP to uncontrolled networks.



Additional resources

The following table points to additional resources you can visit to learn more about the concepts and areas mentioned in this chapter. You can find AskF5 solution articles and the right product manuals for your software version by searching [AskF5 \(support.f5.com\)](https://support.f5.com).

Table 15.1: Additional resources

For more information about	See
Searching BIG-IP iHealth results.	BIG-IP iHealth User Guide
iApps.	DevCentral iApps (devcentral.f5.com/iApps) .
iControl.	DevCentral iControl (https://devcentral.f5.com/wiki/iControl.HomePage.ashx) .
iCall.	DevCentral iCall (devcentral.f5.com/iCall) .
iRules.	DevCentral iRules (devcentral.f5.com/iRules)

Help improve this guide

Please help F5 improve this guide by responding to a few questions about this chapter.

(Note: You must be viewing this document in Adobe Acrobat Reader or similar to use this form.)

Did this chapter answer all of your questions about the subject matter? Yes No

If not, what information should be included that is not? _____

Did you find any errors pertaining to subject matter in this chapter? Yes No

If yes, please describe the error: _____

If yes, please copy and paste the paragraph containing the error here: _____

Did you find non-subject-matter errors in this chapter (spelling, etc.)? Yes No

If yes, please describe the error: _____

If yes, please copy and paste the paragraph containing the error here: _____



Security

At a glance—Recommendations

F5 has identified the following security recommendations:

- Develop system access policy.
- Develop user and password management.
- Policy monitoring for login failures.
- Monitor indications of DoS/DDoS attacks.
- Join the DevCentral Security Compliance Forum.
- Join the security mailing list.

Background

This section provides context for our recommended procedures in the form of overviews and supplemental information.

It includes the following topics:

- Develop a system access policy.
- Develop user and password management.
- Policy monitoring system login activity.
- Monitoring and mitigating DoS/DDoS attacks.

F5 security overview

F5 adheres to industry standard software practices in order to provide software and configurations that are secure by default. F5 investigates and prioritizes security vulnerability reports based on their potential exploitability. Security hotfixes released by F5 for version 9.x and later are cumulative.

When a security hotfix is released, it will contain all other security-related hotfixes and stability-related hotfixes since the last software release. F5 is committed to staying up-to-date on all of the known security vulnerabilities and actively monitors and participates in the following vulnerability databases, all of which it has full membership. These include:

- CERT Coordination Center (CERT/CC).
- CVE (Common Vulnerabilities and Exposures).



F5 actively monitors and responds to the following databases:

- Bugtraq database.
- Redhat Security Mailing List.
- CentOS Security.

Security Updates mailing list

F5 maintains a mailing list for announcements that relate to security issues.

CVE vulnerability

If you would like to determine if your BIG-IP system is vulnerable to a particular CVE, search for the CVE or VU number on AskF5 it the best place to start. F5 Global Support also can field questions about vulnerabilities not covered on AskF5.

If you become aware of a new potential vulnerability in a F5 product, contact F5 Global Support.

In addition, F5 accepts security reports using e-mail at security-reporting@f5.com.

Develop system access policy

F5 recommends the development of a system access policy. This should include, but not be limited to the implementation of a physical security access policy and network access policy.

Physical access policy

F5 recommends operating and housing the BIG-IP system in a secure, access-controlled location, such as a datacenter.

Network access policy

F5 recommends frequent network access policy reviews. At a minimum, the following elements should be verified quarterly or when making changes to the network environment or BIG-IP devices:

Management interface. F5 recommends that you use the management port to provide administrative access to the BIG-IP system. F5 recommends the management interface be connected to only a secure, management-only network, such as one that uses a non-routable RFC1918 private IP address space. See AskF5 article: [SOL7312: Overview of the management port](#).

Port lockdown. The port lockdown security feature allows you to specify particular protocols and services from which the self-IP address defined on the BIG-IP system can accept traffic. The default port lockdown setting is None, which specifies that no connections are allowed on the self-IP address. See AskF5 article: [SOL13250: Overview of port lockdown behavior \(10.x - 11.x\)](#). Ensure that the port lockdown feature only allows access to ports that are necessary for BIG-IP system operation.

Specifying allowable IP ranges for SSH access. You can update the secure shell (SSH) access list from the Configuration utility



and at the command line. See AskF5 article: [SOL5380: Specifying allowable IP ranges for SSH access](#). Note that SSH access should only be granted to administrative user networks.

Configuring an automatic logout for idle sessions. F5 recommends you configure automatic logout for idle sessions for the Configuration utility and SSH. See [AskF5 article: SOL9908: Configuring an automatic logout for idle sessions](#).

Develop user and password management policy

The BIG-IP system provides methods to control and manage user roles, authentication, and passwords. F5 recommends establishing a password policy for the BIG-IP system. This should include strong password requirements and regular audit and removal of inactive accounts in agreement with your corporate policies. For more information about developing a strong password policy see the following AskF5 articles:

[SOL13092: Overview of securing access to the BIG-IP system.](#)

[SOL12173: Overview of BIG-IP administrative access controls.](#)

[SOL13121: Changing system maintenance account passwords \(11.x\).](#)

[SOL4139: Configuring the BIG-IP system to enforce the use of strict passwords.](#)

[SOL5962: Configuring a Secure Password Policy for the BIG-IP System.](#)

[SOL2873: Characters that should not be used in passwords on F5 products.](#)

[SOL13426: Monitoring Login Attempts.](#)

Monitor system login activity

Monitoring login attempts is an important part of network security. Successful and failed login attempts are recorded in the BIG-IP system audit log.

Review system login activity log messages

You can view BIG-IP system login attempts in the Configuration utility and at the command line. For more information, see Event Logging in [BIG-IP TMOS: Concepts](#).

Interpret the audit log

Successful command-line login attempts appear similar to the following example:

```
Mon Jul 6 10:17:38 BST 2014 root 0-0 sshd(pam_audit): user=root(root)
partition=All level=Administrator
tty=/dev/pts/1 host=192.168.10.10 attempts=1 start="Mon Jul 6 10:17:38 2014."
```

When the user logs out, information that appears similar to the following example is reported:

```
Mon Jul 6 10:18:30 BST 2014 root 0-0 sshd(pam_audit): user=root(root)
partition=All level=Administrator
```



```
tty=/dev/pts/1 host=192.168.10.10 attempts=1 start="Mon Jul 6 10:17:38 2014"
end="Mon Jul 6 10:18:30 2014":
```

Unsuccessful command-line login attempts simultaneously generate two messages, as follows: Logged to the **/var/log/audit** file:

```
root 0-0 sshd(pam_audit): User=root tty=ssh host=192.168.10.10 failed to
login after 1 attempts (start="Mon Jul 6 10:19:10 2014" end="Mon Jul 6
10:19:14 2013").:
```

Logged to the **/var/log/secure** file:

```
Jul 6 10:19:14 local/abasm err sshd[24600]: error: PAM: Authentication
failure for root from 192.0.2.10
```

Successful Configuration utility login attempts appear similar to the following example:

```
Mon Jul 6 10:23:23 BST 2014 admin 0-0 httpd(mod_auth_pam):
user=admin(admin) partition=[All]

level=Administrator tty=1 host=192.0.2.10 attempts=1 start="Mon Jul 6
10:23:23 2014."
```

Unsuccessful Configuration utility login attempts appear similar to the following example:

```
Mon Jul 6 10:21:03 BST 2014 bob 0-0 httpd(pam_audit):
User=bob tty=(unknown) host=192.0.2.10 failed to login after 1 attempts
start="Mon Jul 6 10:21:01 2014" end="Mon Jul 6 10:21:03 2014").:
```

To determine why a Configuration utility login attempt failed, log in at the command line and examine the **/var/log/secure** file for a corresponding log entry, similar to the following example:

```
Jul 6 10:21:03 local/abasm err httpd[4133]: [error] [client 192.168.10.10]
AUTHCACHE PAM: user 'bob'

- not authenticated: Authentication failure, referer: https://172.16.10.10/
tmui/login.jsp
```

The previous log entry indicates that the user Bob attempted to log in from 192.168.10.10, but failed to authenticate. If your organization has a SIEM or central monitoring infrastructure this data may be of great use to your corporate security team.

Related products

Advanced Firewall Manager can detect and mitigate many DoS/DDoS attack vectors. For more information see [BIG-IP Systems: DoS Protection and Protocol Firewall Implementations](#) for your software version.

Application Security Manager can detect and mitigate many application targeted DoS/DDoS attacks. For more information see the [BIG-IP Application Security Manager: Implementations](#).

Monitor and mitigate DoS/DDoS attacks

The BIG-IP system default configuration is secure; the system denies all traffic except for traffic types that you specifically



configure the system to accept.

Although the deny-by-default approach protects the resources managed by the BIG-IP system against attacks, remote attackers can initiate DoS / DDoS attacks. DoS and DDoS attacks attempt to make a machine or network resource unavailable to its intended users.

The BIG-IP system provides methods to detect ongoing or previous DoS and DDoS attacks on the system. To detect these attacks, use the procedures described in the following sections.

SYN flood protection

The BIG-IP system includes a feature known as SYN Check, which helps prevent the BIG-IP SYN queue from becoming full during a SYN flood attack. The SYN Check Activation Threshold setting indicates the number of new TCP connections that can be established before the BIG-IP LTM activates the SYN Cookies authentication method for subsequent TCP connections.

When the BIG-IP LTM activates the SYN Cookies authentication method, the system does not need to keep the SYN-RECEIVED state that is normally stored in the connection table for the initiated session. Because the SYN-RECEIVED state is not kept for a connection, the SYN queue cannot be exhausted and normal TCP communication can continue.

Review SYN cookie threshold log messages

The BIG-IP system may log one or more error messages that relate to SYN cookie protection to the `/var/log/ltm` file. Messages that relate to SYN cookie protection appear similar to the following examples:

When the virtual server exceeds the SYN Check Activation Threshold, the system logs an error message similar to the following example:

```
warning tmm5[18388]: 01010038:4: Syncookie threshold 0 exceeded, virtual =  
10.11.16.238:80
```

When hardware SYN cookie mode is active for a virtual server, the system logs an error message similar to the following example:

```
notice tmm5[18388]: 01010240:5: Syncookie HW mode activated, server =  
10.11.16.238:80, HSB modId = 1
```

When hardware SYN cookie mode is not active for a virtual server, the system logs an error message similar to the following example:

```
notice tmm5[18388]: 01010241:5: Syncookie HW mode exited, server =  
10.11.16.238:80, HSB modId = 1 from HSB
```

Modification of SYN cookie threshold

For more information about modifying SYN Cookie Protection configuration see AskF5 articles: [SOL7847: Overview of BIG-IP SYN cookie protection \(9.x - 11.2.x\)](#) and [SOL14779: Overview of BIG-IP SYN cookie protection \(11.3.x - 11.5.x\)](#).



General DoS/DDoS attack vectors

While there are many different DoS/DDoS attack vectors the BIG-IP system protects against without manual configuration, some vectors may require administrative actions to successfully mitigate. This may include but is not limited to the following:

- Configure protocol profile Idle Timeouts.
- Configure TCP profile settings.
- Configure an IP rate class.
- Configure virtual server connection limits Development of iRules for mitigation Modification of other configuration relating to DoS/DDoS mitigation.

For more information about detecting and mitigating DoS/DDoS attacks see AskF5 article: [SOL14813: Detecting and mitigating DoS/DDoS attacks \(11.4.x\)](#).

Adaptive reaper

When a connection is opened to a BIG-IP NAT, SNAT, or virtual server, the BIG-IP unit allocates a chunk of memory for the connection. In order to prevent flooding the BIG-IP unit and to preserve memory, the Adaptive connection reaper closes idle connections when memory usage on the BIG-IP unit increases. The adaptive reaping feature allows the BIG-IP system to aggressively reap connections when the system memory utilization reaches the low-water mark, and stop establishing new connections when the system memory utilization reaches the high- water mark percentage.

Adaptive reaping may be activated by events or conditions that increase memory utilization, including, but not limited to the following:

- Dos/DDoS attacks, in which an attacker attempting to increase BIG-IP memory utilization by sending a large number of connections over a short period of time can cause the system to enter aggressive reaping mode.
- RAM Cache memory allocation.
- Allocating too much system memory for the RAM Cache feature can potentially cause the system to enter aggressive reaping mode to free memory.
- Memory leaks. If a memory leak persists for an extended period of time, the system may enter aggressive reaping mode to free memory.

Review adaptive reaper messages

These events are marked in the `/var/log/ltm` file with messages similar to the following examples:

```
tmm tmm[<PID>]: 011e0002:4: sweeper _ update: aggressive mode activated.  
(117504/138240 pages)
```

```
tmm tmm[<PID>]: 011e0002:4: sweeper _ update: aggressive mode deactivated.  
(117503/138240 pages)
```



The BIG-IP system also generates the following SNMP trap when this event occurs:

```
bigipAggrReaperStateChange.1.3.6.1.4.1.3375.2.4.0.22
```

TMOS based systems do not use Linux memory management for handling traffic, TMM maintains its own memory that should be monitored separately. You can determine the percentage of memory being used by each TMM process on the BIG-IP system using the following command:

```
tmctl -d blade tmm/pagemem
```

Modification of adaptive reaper thresholds

There is generally no need to change these values as they represent an optimal solution for most BIG-IP deployments. Contact F5 Technical Support for assistance in determining the best settings for your solution.

Maximum reject rate log messages

The **tm.maxrejectrate** db key allows you to adjust the number of TCP reset (RST) packets or internet control message protocol (ICMP) unreachable packets that the BIG-IP system sends in response to incoming client-side or server-side packets that cannot be matched with existing connections to BIG-IP virtual servers, self-IP addresses, or Secure Network Address Translations (SNATs). A high number of maximum reject rate messages may indicate that the BIG-IP system is experiencing a DoS/DDoS attack.

Review maximum reject rate log messages TCP

When the number of TCP packets exceeds the **tm.maxrejectrate** threshold, the BIG-IP system stops sending TCP RST packets in response to unmatched packets, and logs an error message.

For example, when the number of packets matching a local traffic IP address (a virtual IP address) or a self-IP address exceeds the **tm.maxrejectrate** threshold, but specify an invalid port; the system stops sending RST packets in response to the unmatched packets and logs an error message to the **/var/log/ltm** file that appears similar to the following example:

```
011e0001:4: Limiting closed port RST response from 299 to 250 packets/sec
```

When the number of packets that match a local traffic IP address (a virtual IP address) and port, or a self-IP address and port, exceeds the **tm.maxrejectrate** threshold, but the packet is not a TCP synchronize sequence number (SYN) packet and does not match an established connection, the system stops sending RST packets in response to the unmatched packets. The system also logs an error message to the **/var/log/ltm** file that appears similar to the following example:

```
011e0001:4: Limiting open port RST response from 251 to 250 packets/sec
```

Internet Control Message Protocol

When Internet Control Message Protocol (ICMP) exceeds the **tm.maxrejectrate** threshold, the BIG-IP system stops sending ICMP unreachable packets in response to unmatched packets, and logs a message to the **/var/log/ltm** file that appears similar to the following example:

```
011e0001:4: Limiting icmp unreach response from 299 to 250 packets/sec
```



Mitigate DoS/DDoS attacks

The BIG-IP system provides features that allow you to mitigate Dos/DDoS attacks on the system. F5 recommends leaving most of the settings at the default levels. However, in the event that you detect an ongoing DoS/DDoS attack, you can adjust the settings using the recommendations in the following sections.

Modification of reject rate thresholds

For more information about modifying Reject Rate configuration see AskF5 article: [SOL13151: Configuring the rate at which the BIG-IP system issues TCP RSTs or ICMP unreachable packets \(11.x\)](#).

Procedures

In addition to maintaining strong authentication and password standards, monitoring login attempts can assist in tracking both authorized and unauthorized attempts to access a BIG-IP controller, giving administrators vital information for formulating a security policy and reacting to threats.

To subscribe to the Security Updates mailing list

1. Go to the [AskF5 Publication Preference Center](https://interact.f5.com/technews.html) (interact.f5.com/technews.html).
2. Type your email address.
3. Select the **Security Updates** check box.
4. Click **Submit**.

Configuration utility

To view login attempts using the Configuration utility

- Go to **System > Logs > Audit > List**.

To view login attempts at the command line

- View the audit log at the command line in the **/var/log/audit** file.



Additional resources

The following table points to additional resources you can visit to learn more about the concepts and areas mentioned in this chapter. You can find AskF5 solution articles and the right product manuals for your software version by searching [AskF5](#) ([support.f5.com](#)).

Table 16.1: Additional resources

For more information about	See
BIG-IP third-party software matrix.	SOL14457: BIG-IP third-party software matrix (11.x).
Overview of the F5 security vulnerability response policy.	SOL4602: Overview of the F5 security vulnerability response policy. This document show how vulnerabilities are assessed by F5 and give pointers on F5 Response policies and communication.
Overview of the F5 critical issue hotfix policy.	SOL4918: Overview of the F5 critical issue hotfix policy. This document covers the policy F5 uses to ensure that fixes for critical issues are disseminated quickly to F5 customers. It also contains links on how to determine which versions of software are currently supported for security fixes.

Help improve this guide

Please help F5 improve this guide by responding to a few questions about this chapter.

(Note: You must be viewing this document in Adobe Acrobat Reader or similar to use this form.)

Did this chapter answer all of your questions about the subject matter? Yes No

If not, what information should be included that is not? _____

Did you find any errors pertaining to subject matter in this chapter? Yes No

If yes, please describe the error: _____

If yes, please copy and paste the paragraph containing the error here: _____

Did you find non-subject-matter errors in this chapter (spelling, etc.)? Yes No

If yes, please describe the error: _____

If yes, please copy and paste the paragraph containing the error here: _____



Optimize the support experience

F5 technical support commitment

F5 strives to continuously improve its support service and create closer customer relationships. Designed to provide assistance with specific break-fix issues and ongoing maintenance of F5 products, F5 professional support services are consistently high-quality.

This means:

- F5 network support engineers conduct themselves professionally at all times.
- F5 is committed to providing the best customer experience possible.
- Customers are treated with respect and given every consideration possible.
- F5 aims to provide resolutions the first time, every time.
- Manager escalation is always available for unresolved or “site down” issues.

Some technical support issues arise from configuration errors, either within the BIG-IP system or with other devices in the network. In other cases, a misunderstanding of BIG-IP capabilities can lead to support questions and issues. Although F5 does everything possible to prevent defects in BIG-IP hardware and software, these issues may still arise periodically. Regardless of the root cause of a problem, the goal is to resolve any issues quickly.

F5 technical support offerings

A variety of technical support offerings are available to provide the right level of support for any organization.

F5 Standard and Premium Support include remote assistance from F5 Network Support Engineers, both online and over the phone.

Premium Plus customers receive priority status at F5, with fast, easy access to a dedicated team of senior-level, F5-certified Network Support Engineers and a Technical Account Manager.

To learn more, see [F5 Technical Support Services](#) or send email to services@f5.com.

Professional services

Take advantage of the full range of F5 Consulting Services to help you design, customize, and implement a solution that is right for your IT infrastructure and which supports your business goals.*

Consulting Services (f5.com/support/professional-services) provides information on a wide range of F5 Professional Services offerings and Professional Services Partners. You can use our online forms to request Consulting Services On Demand for



custom, shorter scope consulting engagements, or iRules OnDemand to get fast access to iRules scripts tailored to your specific needs.

You can make an online request for specific support services by filling out a request form:

Consulting request form (f5.com/support/professional-services/consulting-request-form).

iRules consulting request form (f5.com/support/professional-services/irules-consulting-request-form).

GUARDIAN professional services partners

F5 GUARDIAN Professional Services Partners are authorized as Installation Providers and are also available to assist you. F5 GUARDIANs are selected because they have the skills and experience required to ensure successful implementations of F5 BIG-IP Local Traffic Manager (LTM) and BIG-IP DNS.

See F5 GUARDIAN Professional Service Partners (f5.com/support/professional-services#guardian) for a complete list of partners.

F5 certification

F5 Certified exams test the skills and knowledge necessary to be successful when working with today's application delivery challenges. Our technically relevant and appropriate exams deliver consistently reproducible results that guarantee excellence in those that achieve certification.

Certification levels

The F5 certification program is progressive with the four levels – Administrator, Specialist, Expert and Professional -- building on the skills and knowledge demonstrated on previous exams.

C1 – F5 Certified BIG-IP Administrator (F5-CA)

The starting point for all certifications: a certified BIG-IP Administrator has basic network and application knowledge to be successful in application delivery.

C2 – F5 Certified Technology Specialists (F5-CTS)

The Technology Specialist certification assures employers that the candidate is fully qualified to design, implement, and maintain that specific product and its advanced features.

C3 – F5 Certified Solution Expert (F5-CSE)

The Solution Expert focuses on how F5 technologies combine with industry technology to create real-world business solutions.

C4 – F5 Certified Application Delivery Engineer (F5-CADE)

The Application Delivery Engineer certification exam and requirements are still under development.



C5 – F5 Certified Application Delivery Architect (F5-CADA)

The Application Delivery Architect certification exam and requirements are still under development.

Certificate expiration

F5 certifications are valid for two (2) years. Three months before the expiration date, the holder becomes recertification-eligible and can register for the exam necessary to re-certify. Only the last exam in the highest level certification achieved needs to be retaken.

Certification beta program

We use Beta exams in the creation of all our exams and to maintain their relevancy and accuracy after production. Beta exams are open to all and give candidates an opportunity to have an impact on the Certified program. While Beta exams are twice as long, they cost less than regular exams and give candidates the chance to leave feedback on the exam. Beta exams are critical to our exam development process and a great way to change the Certified program for the better.

Get involved

There are a several ways to get involved with the F5 certification beta program:

- Beta participation. Interested in taking our Beta exams? Contact us at F5Certification@f5.com to learn more.
- Exam development. Contact us at F5Certification@f5.com if you're interested in helping us create our Certified exams.
- LinkedIn community. Join us on [LinkedIn](#) (this link sends you to a external site) for answers to frequently asked questions, community developed resources, and more.

Visit F5-Credential Management System (certification.f5.com) for information or follow the steps to get registered.

Self-help

F5 offers a number of resources to assist in managing and supporting your F5 systems:

- [AskF5 Knowledge Base](#)
- [Downloads](#)
- [Security Updates](#)
- [BIG-IP iHealth®](#)
- [TechNews](#)
- [RSS Feeds](#)
- [DevCentral](#)



- [F5 Global Training Services](#)

AskF5

AskF5 (support.f5.com) is a great resource for thousands of solutions to help you manage your F5 products more effectively and should be the first resource you choose when in need of support. Step-by-step instructions, downloads, and links to additional resources give you the means to solve known issues quickly and without delay, and to address potential issues before they become reality.

Whether you want to search the knowledge base to research an issue, or you need the most recent news on your F5 products, AskF5 is your source for:

Product manuals, operations guides, and release notes.

- F5 announcements.
- General solutions.
- Known issues.
- Security advisories.
- Recommended practices.
- Troubleshooting tips.
- How-to documents.
- Changes in behavior.
- Diagnostic and firmware upgrades.
- Hotfix information.
- Product life cycle information.

Downloads

Downloads are available from the F5 website. It is highly recommended that your F5 software is kept up-to-date, including hotfixes, security updates, OPSWAT updates, BIG-IP ASM Signature files, and Geolocation database updates. All software downloads are available from [F5 Downloads](#) (downloads.f5.com).

Security updates

You can receive timely security updates and BIG-IP Application Security Manager (BIG-IP ASM) attack signature updates from F5. When remote vulnerabilities are discovered, F5 implements, tests, and releases security hotfixes for any vulnerable supported version, and sends an email alert to the F5 Security mailing list. F5 encourages customers with an active support



account to subscribe to this list. For more information, see AskF5 article: [SQL4602: Overview of the F5 security vulnerability response policy](#).

BIG-IP iHealth

The [BIG-IP iHealth \(iHealth.f5.com\)](#) diagnostic viewer is among the most important preventative tools to verify the proper operation of your BIG-IP system. It will ensure hardware and software are functioning at peak efficiency and help detect and address issues that may potentially affect F5 systems. BIG-IP iHealth is not integrated within the BIG-IP system. It is hosted by F5 at [iHealth.f5.com](#) and can be accessed with any web browser.

F5 recommends you generate a BIG-IP iHealth qkview file on the BIG-IP system and upload it to iHealth on a weekly basis in order to benefit from the many regularly occurring diagnostic updates. Uploading qkviews to iHealth also provides F5 technical support with access to your qkviews if you open a support case.

By reviewing the iHealth output, many of the issues commonly experienced by customers can be resolved without the need for opening a support case with F5.

For more information on running BIG-IP iHealth diagnostics, see [BIG-IP iHealth](#).

TechNews

AskF5 provides two TechNews email publications to help keep administrators up-to-date on various F5 updates and other offerings:

- TechNews Weekly HTML eNewsletter includes timely information about known issues, product releases, hot-fix releases, updated and new solutions, and new feature notices.
- TechNews Notifications is a plain-text email that is sent any time a product or hotfix is released. This information is also included in the next weekly HTML TechNews email.

To sign up for the TechNews mailing lists, go to AskF5 ([support.f5.com](#)) and select **Subscribe: Mailing Lists** from the Self-Help menu. Provide your contact information and select **TechNews Weekly Newsletter** and/or **TechNews Notifications**.

AskF5 recent additions and updates

You can subscribe to F5 RSS feeds to stay informed about new documents pertaining to your installed products or products of interest. AskF5 Recent Additions and Updates page provides an overview of all the documents recently added to the Knowledge Base.

Recent Additions and Updates are also published over RSS. You can configure feeds that pertain to specific products, product versions, and/or document sets. You can also aggregate multiple feeds into your RSS Reader to display one unified list of all selected documents.

To generate an RSS feed, go to [AskF5 Knowledge Base](#) and select **Subscribe: RSS** from the **Self-Help** menu.



DevCentral

[DevCentral](https://devcentral.f5.com) (devcentral.f5.com) is an online forum of F5 employees and customers that provides technical documentation, discussion forums, blogs, media and more, related to application delivery networking. DevCentral is a resource for education and advice on F5 technologies and is especially helpful for iRules and iApps® developers. Access to DevCentral is free, but registration is required. As a DevCentral member, you can do the following:

- Ask forum questions.
- Rate and comment on content.
- Contribute to “wikis.”
- Download lab projects.
- Join community interest groups.
- Solve problems and search for information.
- Attend online community events.
- View educational videos.

F5 global training services

F5 Global Training Services provides traditional classroom learning opportunities, live-online training, and free, self-paced online courses to help you get the most out of your investment.

In-person courses

F5 courses are available in multiple training facilities across five continents. Each one combines instructor presentations, classroom discussions and interactive labs. The hands-on learning environment helps provide a fast track to accomplishing your goals.

Virtual instructor-led training

Remote on-line courses mirror classroom training. Participants watch the remote instructor’s live lecture online, participate in discussions, and do lab exercises using remote desktop control.

Free online training

You can use the self-paced Getting Started series of free, web-based courses to learn how to deploy F5 solutions to address your most common application delivery problems:

For more information about F5 education opportunities at F5, go to f5.com/education.

F5 Training Programs and Education (f5.com/education/training) provides links to course schedules, pricing, and registration details. It also has information about alternative training solutions such as virtual and web-based training for those who cannot



attend training in person. Links to more information are provided at this site for those interested in F5 Professional Certification or a non-accredited Application Delivery Networking Certificate through F5 and the University of Phoenix.

Engage Support

F5 Technical Support is designed to provide support for specific break-fix issues for customers with active support contracts. For more information about F5 scope of support, see [Support Policies](#) on [F5.com](#).

Options for assistance

You can contact F5 Support in two ways:

Online: You can open a support case at the [F5 WebSupport Portal](#). Click **Register for an Account** to access to the WebSupport Portal.

By phone: Phone numbers are provided in the General contact numbers section below. It is strongly recommended that you contact F5 by phone if you have a Sev1 or Sev2 case, as defined in [Opening a Support Case](#).

F5 technical support resources

F5 support resources are available **24 hours** a day, seven days a week, and are distributed around the globe in multiple support centers. Live technical support is provided by our professional Network Support Engineers. Hours of availability may vary depending on the service contract with F5.

Contact numbers

Standard, Premium, and Premium Plus Support customers can open and manage cases by calling one of the contact numbers listed below.

North America

North America: 1-888-882-7535 or (206) 272-6500

Traffic[®] Support Only: 1-855-849-5673 or (206) 272-5774

Outside North America

Outside North America, Universal Toll-Free: +800 11 ASK 4 F5 or (800 11275 435)

Additional contact numbers by country

Australia: 1800 784 977

China: 010 5923 4123

Egypt: 0800-000-0537

Greece: 00-800-11275435



Hong Kong: 001-800-11275435

India: 000-800-650-1448; 000-800-650-0356 (Bharti Air users)

Indonesia: 001-803-657-904

Israel: 972-37630516

Japan: 81-3-5114-3260 or 0066-33-812670

Malaysia: 1-800-814994

New Zealand: 0800-44-9151

Philippines: 1-800-1-114-2564

Saudi Arabia: 800-844-7835

Singapore: 6411-1800

South Africa: 080-09-88889

South Korea: 002-800-11275435

Taiwan: 00-800-11275435

Thailand: 001-800-12-0666763

United Arab Emirates: 8000-3570-2437

United Kingdom: 44-(0)8707-744-655

Vietnam: 120-11585

Open a support case

F5 provides several resources to help find solutions to problems. Before opening a support case with F5 technical support, check to see if the issue you are encountering is already documented.

The following is a list of resources to consult before opening a support case with F5:

[Deployment guides](#) and [white papers](#) provide information about specific deployment configurations.

[AskF5 Knowledge Base](#) provides many articles including known issues, how-to guides, security issues, release notes, and general information about products. Many of the issues customers encounter are already documented on this site.

[BIG-IP iHealth](#) enables customers to upload qkview configuration snapshots in order to verify operation of any BIG-IP system.

Gather information to open a support case



If your issue cannot be solved using the resources listed, and you need to open a support case, you must first gather several pieces of important information about your issue. Providing full and accurate information will help speed the path to resolution. The required information for the majority of situations is summarized below:

The serial number or base registration key of the specific BIG-IP system requiring support. For more information, see AskF5 article: [SOL917: Finding the serial number or registration key of your F5 device](#).

A full description of the issue. A clear problem statement is the best tool in helping to troubleshoot issues. Your description should include as much of the following information as you can provide.

Occurrences and changes: The date and times of initial and subsequent recurrences. Did this issue arise at implementation or later? Were there any changes or updates made to the BIG-IP system prior to the issue arising? If so, what were they?

Symptoms: Ensuring your list of symptoms is as detailed as possible will give more information for support personnel to correlate with.

Scope of the problem: Note whether the problem is system-wide or limited to a particular configuration feature, service, or element (such as VLAN, interface, application service, virtual server, pool, and so on).

BIG-IP component: The feature, configuration element, or service being used when the problem occurred (for example: portal access, network access, authentication services, VDI, Exchange).

Steps to reproduce: The steps to reproduce the problem as accurately and in as much detail as possible. Include expected behavior (what should happen) as well as actual behavior (what does happen).

Errors: Complete text of any error messages produced.

Environment: Current usage of the system. (Is this unit in production? If so, is there currently a workaround in place?)

Browsers: Types and versions, if applicable.

Changes: System changes made immediately prior to the problem's first occurrence. This may include upgrades, hardware changes, network maintenance, and so on. Have any changes been made to resolve the problem? If so, what were they?

Issue Severity: A description of the impact the issue is having on your site or Case severity

- Severity 1: Software or hardware conditions on your F5 device are preventing the execution of critical business activities. The device will not power up or is not passing traffic.
- Severity 2: Software or hardware conditions on your F5 device are preventing or significantly impairing high-level commerce or business activities.
- Severity 3: Software or hardware conditions on your F5 device are creating degradation of service or functionality in normal business or commerce activities.
- Severity 4: Questions regarding configurations ("how to"), troubleshooting non-critical issues, or requests for product



functionality that are not part of the current product feature set.

- Contact and availability information including alternate contacts authorized to work on the problem with F5 Technical Support. When there are more personnel available to work with F5 Technical Support, the resolution of your issue may be expedited.
- Remote access information, if possible.
- A qkview file obtained while problem symptoms are manifesting. A qkview of the system before the occurrence is also useful. F5 recommends archiving qkviews regularly. For more information, see [BIG-IP iHealth](#).
- Product-specific information: Software versions and types of equipment in use.
- Platform and system. Version and provisioned software modules of the affected system.

To locate platform and system information using tmsh from the command line

- Type the following command:

```
tmsh show /sys hardware
```

Output will appear similar to the following example:

```
<SNIP some of the output>
```

```
Platform
```

```
Name BIG-IP 3900
```

```
BIOS Revision F5 Platform: C106 OBJ-0314-03 BIOS (build: 010) Date: 02/15/12
```

```
Base MAC 00:01:d7:be:bf:80
```

```
System Information
```

```
Type C106
```

```
Chassis Serial f5-jspv-lzxw
```

```
Level 200/400 Part 200-0322-02 REV C
```

```
Switchboard Serial
```

```
Switchboard Part Revision
```

```
Host Board Serial
```

```
Host Board Part Revision
```

To copy software version and build number information from the command line

1. Type the following command:

```
cat /VERSION
```

Output will appear similar to the following example:

```
Product: BIG-IP
```



```
Version: 11.6.0
Build: 0.0.401
Sequence: 11.6.0.0.0.401.0
BaseBuild: 0.0.401
Edition: Final
Date: Mon Aug 11 21:08:03 PDT 2014
Built: 140811210803
Changelist: 1255500
JobID: 386543
```

2. Highlight and copy the output information and include it with your support case.

To copy provisioned module information from the command line

1. Type the following command:

```
tmsh list /sys provision
```

Output will appear similar to the following example:

```
sys provision afm { }
sys provision am { }
sys provision apm {
level nominal
}
sys provision asm { }
sys provision avr { }
sys provision fps { }
sys provision gtm { }
sys provision lc { }
sys provision ltm {
level minimum
}
sys provision pem { }
sys provision swg { }
```

2. Highlight and copy the output information and include it with your support case.

Open a case using WebSupport Portal

If you cannot find the answer to your problem using the resources listed above, you can open a support case online, using the F5 WebSupport Portal (websupport.f5.com).



Use of the WebSupport Portal requires a current support contract and registration on the F5 website (login.f5.com).

To request access during registration, select I have a support contract and need access to WebSupport. You will be prompted to enter your registration key or serial number. Once registered, you'll receive an email within 24 hours letting you know your account has been enabled with WebSupport Portal access.

To register for WebSupport portal access

1. Go to [F5 WebSupport portal](#).
2. Click **Register for an Account**.
3. Enter your email address.
4. Complete the **Contact information** portion of the page and then select **I have a support contract and need access to WebSupport**.
5. Enter your **Serial Number** or **Registration Key** (optional).

After you have logged-in you are ready to open a support case.

Send information to Support

Once the information is assembled and appropriate documentation gathered, transfer it to F5 technical support following the steps in [Share diagnostic files with F5 technical support](#). For more information, see AskF5 article: [SOL2486: Providing files to F5 Technical Support](#).

Share diagnostic files with F5 technical support

F5 technical support may require diagnostic files to help resolve technical support issues. Upload files to F5 using one of the following two methods:

- Upload qkview diagnostic files to [BIG-IP iHealth](#) (ihealth.f5.com).
- Upload/downloading files using dropbox.f5.com.

Upload qkview diagnostic files to BIG-IP iHealth

The preferred method for providing a qkview diagnostic file to F5 Support is to upload the file to the BIG-IP iHealth website. BIG-IP iHealth allows you to quickly diagnose the health and proper operation of your BIG-IP system. For more information about using BIG-IP iHealth, see [BIG-IP iHealth](#).

Upload/download files using dropbox.f5.com

The dropbox.f5.com site is a widely available file repository for exchanging incoming and outgoing diagnostic files with the F5 Technical Support team. The dropbox.f5.com site supports HTTP, FTP, and SFTP for transferring files to F5, and FTP and SFTP



for retrieving files from F5.

Username and password

Access to the dropbox.f5.com site is associated with an open support ticket number with syntax CXXXXXX or 1-#####. The username provided to the dropbox.f5.com site is the ticket number, and the password provided is an email address of a user associated with the ticket.

For example, if joeuser@example.com has opened ticket C123456, he would log in to the dropbox.f5.com site using the following information:

Username: C123456

Password: joeuser@example.com

If joeuser@example.com has opened ticket 1-12345678, he would log in to the dropbox.f5.com site using the following information:

Username: 1-12345678 Password: joeuser@example.com

For additional information regarding uploading and downloading files using dropbox.f5.com, see [AskF5 article SOL2486: Providing files to F5 Technical Support](#).



Legal Notices

Trademarks

AAM, Access Policy Manager, Advanced Client Authentication, Advanced Firewall Manager, Advanced Routing, AFM, APM, Application Acceleration Manager, Application Security Manager, ARX, AskF5, ASM, BIG-IP, BIG-IQ, Cloud Extender, CloudFucious, Cloud Manager, Clustered Multiprocessing, CMP, COHESION, Data Manager, DevCentral, DevCentral [DESIGN], DNS Express, DSC, DSI, Edge Client, Edge Gateway, EdgePortal, ELEVATE, EM, Enterprise Manager, ENGAGE, F5, F5[DESIGN], F5 Certified [DESIGN], F5 Networks, F5SalesXchange [DESIGN], F5Synthesis, f5Synthesis, F5Synthesis[DESIGN], F5 TechXchange [DESIGN], Fast Application Proxy, Fast Cache, FirePass, Global Traffic Manager, GTM, GUARDIAN, iApps, IBR, Intelligent Browser Referencing, Intelligent Compression, IPv6 Gateway, iControl, iHealth, iQuery, iRules, iRules OnDemand, iSession, L7 RateShaping, LC, Link Controller, Local Traffic Manager, LTM, LineRate, LineRate Systems [DESIGN], LROS, LTM, Message Security Manager, MSM, OneConnect, Packet Velocity, PEM, Policy Enforcement Manager, Protocol Security Manager, PSM, Real Traffic Policy Builder, SalesXchange, ScaleN, Signalling Delivery Controller, SDC, SSL Acceleration, software designed applications services, SDAC (except in Japan), StrongBox, SuperVIP, SYN Check, TCP Express, TDR, TechXchange, TMOS, TotALL, Traffic Management Operating System, Traffix Systems, Traffix Systems (DESIGN), Transparent Data Reduction, UNITY, VAULT, vCMP, VE F5 [DESIGN], Versafe, Versafe [DESIGN], VIPRION, Virtual Clustered Multiprocessing, WebSafe, and ZoneRunner, are trademarks or service marks of F5 Networks, Inc., in the U.S. and other countries, and may not be used without express written consent.

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

Patents

This product may be protected by one or more patents. See the [F5 Patents](http://www.f5.com/about/guidelines-policies/patents) page (<http://www.f5.com/about/guidelines-policies/patents>).

Notice

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

Publication Date

This document was published in November 2015.

Publication Number

BIG-IP TMOSOps - 02_0



Copyright

Copyright © 2013-2015, F5 Networks®, Inc. All rights reserved.

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 by applicable user licenses. F5 reserves the right to change specifications at any time without notice.

Appendix A: Outside the Box

The following appendices, while not directly relevant to BIG-IP operations and maintenance, detail features of BIG-IP box and strong data center practices suggested by F5.

Front panel characteristics



Figure A.1 BIG-IP 5000 series platform front panel

Although the physical layout of F5 application delivery controllers varies, they typically share some common front panel features, as shown in Figure A.1.

These features include:

1. Management interface.
2. USB ports.
3. Console port.
4. Failover port.
5. Indicator LEDs.
6. LCD panel.
7. LCD control buttons.
8. TMM switch interfaces.

On newer application delivery controllers, the serial number is on the front panel, underneath the LCD display. On older devices, it is located on the back or side panel.



Note The VIPRION 2000 Series platform features an external USB LCD module.



Network connection entry points and traffic types

The BIG-IP system uses two types of network connection entry points:

- Management interface (MGMT).
- TMM switch interfaces.

Either the TMM switch interfaces or the MGMT interface can provide administrative access to the BIG-IP system. However, F5 recommends that you use the management port. The TMM switch ports are the interfaces that the BIG-IP system uses to process application traffic. The MGMT interface is intended for administrative traffic only, and cannot be used for application traffic.



Note For more information about operational activities relating to the MGMT interface and TMM switch interfaces, see [Networking and Cluster Health](#).

Console port

On older platforms, the console port is configured with a 9-pin serial port; on new platforms, the console port is configured with an RJ-45 port.

On 9-pin serial port platforms, you must use a properly constructed null modem cable to connect the 9-pin serial port to a serial console device. Pre-fabricated null modem cables with various connectors are available from many sources, but you must verify the pinouts on each to ensure that they comply with the established standards.

For more information on both pinouts see AskF5 articles:

- [SOL587: Pinouts for serial terminal cables used to connect the 9-pin serial port on F5 products.](#)
- [SOL13644: Pinouts for the RJ-45-based console cable and adapter for F5 products.](#)
- [SOL9156: Setting the baud rate of the serial console port \(9.x-10.x\).](#)



Note F5 recommends that you connect to the console port for administrative access and console logging. When connected to the console port, you can still monitor activity on the system and carry out troubleshooting activities should you lose network access to your BIG-IP system or experience daemon failures.



Failover port (hardwired failover)

In a Device Service Cluster, up to eight BIG-IP systems (hardware or VE) can be connected together for the purposes of synchronizing their configurations and failing over to one another under certain conditions. By default, the BIG-IP systems use heartbeat packets sent over the network to communicate their availability and their active or standby status.

BIG-IP hardware platforms offer the option to connect two devices together in an active-standby device service cluster (a.k.a. redundant pair), and to allow hardwired failover to occur between the devices. (A VIPRION platform does not support hardwired failover, nor is hardwired failover available for any device service cluster with more than two devices.) Hardwired failover is also based on heartbeat detection, where the standby BIG-IP unit continuously sends a signal to the active unit in the pair along an RJ-45 or 9-pin serial cable strung between the two units. If a response does not initiate from the active BIG-IP unit, failover is triggered. When BIG-IP redundant devices connect using a hardwired failover cable; the system automatically enables hardwired failover.



Note Network failover is a requirement for an active-active device service cluster. An active-active pair must communicate over the network to indicate the objects and resources they service. Otherwise, if network communications fail, the two systems may attempt to service the same traffic management objects, which could result in duplicate IP addresses on the network.

Even if you configure hardwired failover, communication over the network is necessary for certain features to function properly, for example, the communication that occurs over the network during failover mirroring.



Note On active-standby device service clusters (two devices only), F5 recommends that you use hardwired failover in tandem with network failover wherever possible. For more information, see AskF5 article: [SOL2397: Comparison of hardwired failover and network failover features](#).



LCD panel and LED indicators

Using the LCD panel and its associated control buttons, you can do management tasks on a BIG-IP or VIPRION platform without attaching a console or a network cable. (See Figure A.2.)



Figure A.2 LCD panel on a BIG-IP 7000 series application delivery controller

The functionality of the LCD menus varies from platform to platform, but the following parameters apply:

- You can use the Options or Config menu to adjust the display properties of the LCD panel.
- On BIG-IP platforms, you can use the System menu to view options for rebooting, halting, and “netbooting” the hardware, and for configuring the management interface.
- On VIPRION platforms, you can use the System menu to configure the management interface on both clusters and blades, and to configure various options for the hardware.
- You can use the Screens menu to specify the information that is displayed on the default screens.

BIG-IP systems generally have four indicator LEDs on the LCD panel, while VIPRION platforms include indicator LEDs in many locations.

For example, the VIPRION 4800 platform includes indicator LEDs on the LCD panel, on the individual blades, on the power supplies, on the fan tray, and on the annunciator cards. The meaning of each indicator LED can vary from platform to platform, and details are provided in the associated Platform Guide.

Find a platform guide

To find the appropriate guide for your BIG-IP or VIPRION platform

1. Find platform number on the front panel of the device.
2. Go [AskF5 \(support.f5.com\)](https://support.f5.com).

3. In the **Search** field, type:

```
<platform number> platform guide
```

Clear the LCD and the alarm LED remotely

In some cases, it may be desirable to clear LCD warnings and the Alarm LED remotely. Performing this action may prevent onsite personnel from discovering and reporting an old warning, or having to teach the onsite personnel how to clear the LCD.



Note For instructions on how to clear the LCD and the Alarm LED remotely, see AskF5 article: [SOL11094: Clearing the LCD and the Alarm LED remotely](#).

Back panel characteristics



Figure A.3 BIG-IP 5000 series platform back panel

As with the front panel, the back panel layout varies from platform to platform. Figure A.3 shows the back panel on a BIG-IP 5000 series, which features:

1. Power input panel 1 (power switch and power receptacle).
2. Power blank.
3. Chassis ground lug.

Some platforms, such as the BIG-IP 7000 Series, feature dual power inputs (switches and receptacles), as shown in Figure A.4. Some platforms, such as the BIG-IP 10000 Series, have power receptacles but no power switches, as shown in Figure A.5.



Note Platforms with no power switches are powered on/off by connecting/disconnecting the power plug.



Figure A.4 BIG-IP 7000 series platform back panel with two (redundant) power inputs (switches and receptacles)



Figure A.5 BIG-IP 10000 series platform back panel with two power receptacles and no power switches



VIPRION chassis characteristics

The VIPRION platform includes two primary components: the chassis and blades, which reside within the chassis and provide the hardware and software needed to manage network traffic.

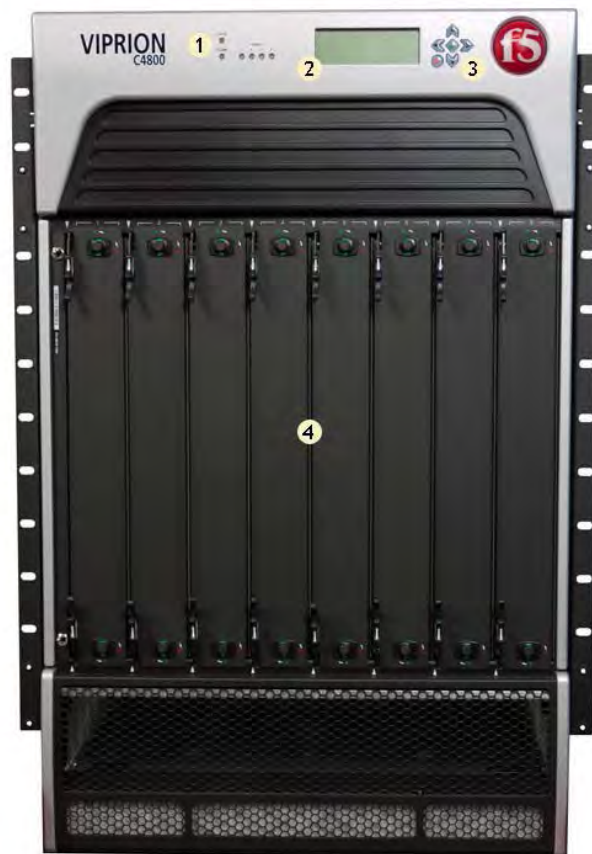


Figure A.6: VIPRION 4800 Platform chassis components

Although the location varies from chassis to chassis, in general a VIPRION chassis includes:

1. Indicator LEDs (system and power status).
2. LCD display.
3. LCD control buttons.
4. Blanks for blades.



Note The VIPRION 2000 Series platform features an external USB LCD module.

VIPRION blade characteristics

A blade is the primary component that handles the traffic management within the VIPRION platform and the number of blades supported varies by VIPRION chassis. For example, you can install up to eight blades in a VIPRION 4800 Series chassis. These blades comprise a group, known as a cluster. The chassis includes blanks in the slots where blades are not installed.

Blanks must be installed in all unused slots, as they help ensure proper airflow within the chassis and EMI compliance of the unit.



Figure A.7 VIPRION B4300 blade components

A VIPRION blade contains many of the same elements as a BIG-IP platform front panel, including:

1. Compression screw.
2. Blade indicator LEDs.
3. Management port.
4. USB ports.
5. Console port.
6. Failover port.
7. TMM switch interfaces.
8. Interface indicator LEDs.



Appendix B: Deployment and Response Methodologies

At a glance—Recommendations

This appendix outlines strategies for managing updates and handling issues for your BIG-IP systems, including:

- Change and revision control.
- Testing and validation.
- Response methodologies.
- Incident handling.
- Root-cause analysis (RCA).

Throughout the rest in this guide are prescriptive tasks with detailed instructions for executing them. This chapter will instead focus on providing an overview of processes and tools that can be employed to make working with BIG-IP systems, and your application delivery environment as a whole, more manageable.



Note In this chapter, we will be providing general guidance and recommendations, but are intentionally leaving the details up to the individual customer. There is no one way to identify, step-by-step deployment and response methodologies in all cases. It is up to you to determine the methods that provide the best fit for your organization. For assistance with deployment, contact F5 Consulting Services or your F5 sales representative.



Background

This section provides context for our recommended procedures in the form of overviews and supplemental information.

Change and revision control

This section briefly covers practices for configuration management, which are not necessarily specific to BIG-IP systems, as they are based on common methodologies and tools used throughout the networking industry. The goal of each is to provide some level of regulation and/or tracking of changes in the environment.

Inadequate or poorly-documented change control practices continue to plague the industry. Such change and revision control of information is invaluable to troubleshooting efforts, and is critical in cases where a root-cause analysis (RCA) is necessary. For more information, see Root-cause analysis and Support files sections of this appendix.

Throughout this section, the term “environment” is used to represent all systems and components that are involved in the delivery of essential business processes or services.

Change control

Change control is a strategic and proactive process designed to ensure system changes are carried out in a controlled and coordinated manner. It is the process of peer-based review and approval of changes to the environment, is implemented in the form of business processes, and is driven by people and not technology.

The benefits of an effective change control process include:

- Organizing and monitoring changes during deployment.
- Clarifying the possible impacts of changes to your production environment.
- A repeatable and accountable decision-gate that documents all changes made to the environment.
- Consolidating changes into a single maintenance period reduces the frequency and impact of service interruptions.

Although change control processes vary by software development lifecycle (SDLC) methodology, industry standards and organizational maturity, most contain one or more of the following phases or gates:

- Request: A record of who is requesting the change and why (importance, impact and complexity)
- Evaluation/triage: A formal stakeholder review of the requests with evaluation of risks, business benefits, impact and so on. Results of evaluations are documented and made public for broader review.
- Planning/scheduling: Approved requests are scheduled to maintenance period and published to stakeholders.
- Testing: Dry runs of new processes are done and software is testing on a non-production environment. A preproduction environment is strongly recommended.



If such an environment is not available, code should be documented, peer reviewed and evaluated for system impact. Formal “sign off” of such testing and reviews should also be retained.

- Implementation: Images and backups of data, logs and so on. are archived prior to implementation and system health baselines such as BIG-IP iHealth qkview is taken. All change documented in a change log and any anomalies recorded.
- Acceptance and close: Acceptance testing or some other method of evaluating the success of the change should be done. Completions of changes are documented and post-mortems for both successful and less successful maintenance activities is done on regular basis.

Revision control

Revision control is a tactical and reactive process of tracking the history of changes that have been made to the environment, but unlike change control, is driven by technology and not people.

The benefits of an effective revision control process include:

- A clear historical record of changes to provide faster identification, diagnosis, and resolution of change-related issues is defined.
- Multiple levels of “roll-back” capability defined for immediate circumvention of unforeseen change-related issues.
- Revision control is particularly important when BIG-IP APIs and Automation Interfaces are employed and when changes to configuration templates and files are made. This work product should be held to the same standards of any other software development project.

As BIG-IP system customizations are developed and deployed; some customers have accidentally deployed differing versions of the same code into their various BIG-IP environments. Such occurrences can negatively effects on the BIG-IPs system's performance and thwart the intent of the customization.

Some revision control systems also provide methods for preventing “concurrent access” problems, by simply locking files so that only one developer has “write access” to the central “repository.” Although controversial, this can prevent problems, such as one developer overwriting the changes made by another. Such occurrences can also result in unintended consequences.

The minimum revision control process should require developers and system administrators making changes to:

- Retain multiple copies of each version of a script or file.
- Appropriately label all scripts and files.
- Archive all scripts and files in a secure location.

Change control vs. revision control

Having a change control process does not automatically mean that a revision control process must also be in place, and vice versa, but there are clear benefits to using them in tandem. But, change control implies that revision control is also in place,



since the effort required to record the history of changes after taking the time to review and validate them is insignificant. However, it is entirely possible, and even desirable in some circumstances, to have revision control implemented without any change control.

At a minimum, F5 strongly recommends using revision control when administering BIG-IP systems. Ideally, all other systems on the networks that your BIG-IP devices communicate with (and integral to your application delivery network) would also be under revision control, such as routers, switches and servers. Having a history of changes to the BIG-IP systems and the wider environment provides essential diagnostic and troubleshooting information. Without this information, many types of issues and events cannot be fully investigated, nor is their potential impact fully understood, since there is no way to correlate changes in behavior or service with changes in configuration of the systems involved.

In all cases, revision control increases the speed and effectiveness of investigative efforts. The most valuable gain, however, is the ability to “roll-back” or revert previous changes, which can be invaluable should it be discovered one of them is the source or trigger of an issue.

Depending on the needs of your organization, change control can be implemented as a process around the revision control system. While revision control tracks the history of changes, and provides a better system for recovery from erroneous changes, change control acts as a gatekeeper, providing a “go/no-go” decision determining whether changes are deployed into the environment.

For example, minor changes (those with little or no business and/or technical impact to the environment) can be consolidated and implemented simultaneously within a maintenance period, without the need for a rigorous approval process. Significant changes (those with greater business and/or technical impact) can be peer-reviewed, and approved by a change control/gatekeeper function before being allowed into the environment.

Having a controlled stream of changes into the environment helps make it very clear if issues or undesirable events are related to a specific change or set of changes, and serves to remove all randomization from the environment.

Recommendations and examples

F5 advises that one or both control systems—change and/or revision—are used in the course of administering BIG-IP products, but does not advocate any particular system or process. Every customer environment is unique, and only you will know what is best for your application delivery needs.

While primarily used for source code management, these tools have the ability to track changes to data of all kinds.



Revision control systems

Some examples of popular revision control systems include:

- Git
- Mercurial
- PERFORCE
- SVN

Change control process

For this example, we will assume a team of three administrators: Alice, Bob, and Charlie.

Alice has finished testing a new configuration on a test BIG-IP VE; she decides it is ready for introduction into the production environment. Alice checks her change into the revision control system, so that it can be moved into production.

Once a week, on Thursday, all unimplemented changes in revision control are reviewed in a team triage with Alice, Bob and Charlie. Each revision is discussed and a collective decision is made whether to approve each change and allow it into the environment, defer the change to a later date pending specific updates or modifications for further review, or outright reject the change. An alternative to a team triage is simple peer-review, as implemented in source code development, where Alice asks Bob or Charlie to review and sign-off on her change. In both cases, the goal is to have each change double-checked before it can move on.

Once a week, on Monday morning, all approved changes are pushed into production. Alice, Bob and Charlie are all on hand to monitor the deployment. Any new issues they find throughout the week can be more easily tracked back to a specific change, since there is a clear history of what has been modified.

Testing and validation

As important as change and revision control are to the application deployment life cycle, proper testing and validation of environment changes is equally key. Configuration changes to a BIG-IP system are no exception. In this section, we will provide some high-level recommended practices, along with examples of what that might look like.

There are many different ways to ensure proper vetting of configuration changes before they are deployed. All of methods require some type of tiered environment where testing can be done.

Levels in a tiered deployment environment

Production

The production environment directly serves customers, employees, and other users of your business processes and application services. It is sometimes referred to as the “live” environment or simply as “production”, and can be viewed as the top tier in the application delivery environment. F5 strongly suggests that changes never be made directly in “production.”



Staging

The staging environment is secondary to the production environment, and generally the last stop in any testing tier. Sometimes referred to as “pre-production”, it may support a subset of production users who are involved in acceptance testing, or serve as a standby or overflow area for the production environment. It is the last stop for validating changes before they are introduced into production. As such, the staging environment should be a direct clone or “mirror” of the production environment in order to mimic the complete production application delivery experience.

Sandbox

The sandbox environment, one of the lower tiers in testing, is also frequently modeled after the production environment, but is closer to the developers and administrator than the user. It is often implemented as a virtual machine (using BIG-IP VEs) or as an isolated lab network.

Why a tiered testing approach?

Separate tiered environments for testing, pre-production validation (staging), and production deployment helps checkpoint changes before they reach your critical business users, dramatically decreasing the impact on business processes and other technology systems. It also reduces the time required for problem resolution as problems can be reproduced and diagnosed external to your production application delivery network.

The Change deployment life cycle

Development sandbox

The life cycle for changes actually begins in the sandbox, which can be as simple as a BIG-IP VE on an individual workstation or as complex as a small-scale duplication of production, complete with performance and functional testing suites. The sandbox is where changes can be evaluated free of consequence to critical production business processes, and the number of variables can be controlled for detailed analysis of behavior.

Application design and testing is often done on an isolated network in a very specific, non-user environment. All too often, applications behave completely differently in production simply because they were not tested or built in the same environment where they are ultimately deployed. In a perfect world, all deployments would have a complete sandbox that mirrors production, and performance/functional testing would be ongoing. Due to capital and operational constraints, however, this is not always possible. Having a minimal sandbox capability, even as basic as BIG-IP VE on individual workstations, will provide significant benefit as a testing and experimentation area.

As portable virtual machines running on any VMware server-based platform, virtual BIG-IP instances can be integrated into application architecture planning and design stages. This gives application architects access to the application tools available in all BIG-IP appliances—such as application acceleration and optimization policies, security policies, and F5 iRules control language.

In this model, BIG-IP virtual edition products can be used as a “pre-development” tool for new applications. Many parts of the organization may not have access to physical BIG-IP hardware during application design and testing, but anyone can download



trial versions of virtual BIG-IP instances and deploy them with their application as part of design and testing. This means that designers and integrators can evaluate the interaction between the BIG-IP devices and the new application to assess and maximize the benefits long before application staging and production. Downloads of trial F5 project can be found at [F5 Product Trials \(f5.com/products/trials/product-trials\)](https://f5.com/products/trials/product-trials).



Note F5 also offers BIG-IP VE in the cloud through the Amazon Market Place. VMs are available on a “Bring Your Own License” (BYOL) or hourly/annual subscription basis.

Staging in pre-production

Much like the design stage, testing is usually done in a quarantined part of the network called the staging environment. In a staging environment, however, applications often act differently than they will in production because they are tested under artificial, simulated circumstances.

Staging provides similar functions to the sandbox, but instead of being a confined environment is reachable directly along-side production. This is often accomplished using a more-or-less full- scale duplication of the production network, and then exposed using a separate DNS zone. Beta versions of websites are a good example of this concept in action. Administrators can do functional testing as though they were a real client, or it can be used as part of a “phased deployment” paradigm.

In some operational models, a purely virtual solution is most practical. By building BIG-IP Virtual Edition products into the staging environment during QA testing, IT staff can more accurately measure and size the application for real-world deployment, in essence, mirroring the production deployment without negatively affecting production traffic and applications.

Testing and QA is the best time to customize BIG-IP application policies. BIG-IP application and policy templates start with customized network delivery configurations for well-known applications such as Microsoft Exchange Server, SAP Dynamics, LDAP, and RADIUS. Using BIG-IP LTM VE, for example, the templates can be further refined to provide a specific delivery environment for the application before it is moved into production. During this time, iRules can be written and tested with the application to measure the effect on both the application and on BIG-IP Virtual Edition products.

With easy access to a full-featured, portable BIG-IP virtual platform, everyone involved in the application design and deployment has the opportunity to build application delivery networking features into the application life cycle from the beginning.

Going live

Finally, changes make their way into the production environment, and are “live.” This can come in the form of changes being pushed from staging or the revision control system to production, or as a migration of the staging environment into production as shown in the Phased Deployment example.

As the application is moved into production, BIG-IP Virtual Edition products enable the application delivery life cycle to be completed under two different models. In both, successful production deployments for BIG-IP virtual instances depend on deploying the BIG-IP virtual environment along with the physical environment, either in a stand-alone architecture or as part of a larger enterprise cloud deployment.



Test and development configurations, settings, iRules, and templates for virtual BIG-IP instances can be moved onto physical BIG-IP appliances as new applications are rolled into production. These application-specific configuration changes can be quickly tested and validated to work in a production environment, drastically reducing the time needed to build new production configurations.

In a truly fluid and agile environment, especially one where the new applications are also running on virtual platforms, BIG-IP virtual instances can be bundled with the application and pushed live to production at the same time. This model treats BIG-IP virtual instances as an integral and required part of the application rollout, pushing the vADC as well as the pre-configured application policy templates—fine-tuned during development, test, and staging—into production together.

By incorporating BIG-IP, virtual edition products into planning for deployments of production applications, application architects, designers, and developers can see real-world production scenarios at every step of the application life cycle.

Example: phased deployment

Alice, Bob, and Charlie are the three network administrators of a small website application. They manage the entire infrastructure, but the content is delivered by a different team that has direct access to the servers for publication. Alice tests her optimizations of one of the core iRules using a BIG-IP VE in a shared lab environment that is configured to be equivalent to production.

Once Alice has finished testing her modifications, she publishes them to the revision control system. Simple repository automation immediately publishes her updates to their staging network, which they call pre-production. It is a portion of their production environment dedicated to staging. Upstream DNS/routing (or a BIG-IP using iRules) begins to slowly migrate production traffic into pre-production at a controlled rate; Alice and her team let it “bleed over” 10% of pre-production capacity every **5 minutes**. Alice and her team observe their monitoring and logging systems during this time, looking for any errors, alerts or unexpected behavior. Once the pre-production environment has sustained production traffic levels for a set length of time, the change is deemed stable.

Traffic is migrated out of pre-production until the staging network is once again free of production traffic. Alice’s change is published to production, and the pre-production environment is re-cloned from production. Alice and her team are ready to submit and validate further changes.

Response methodologies

In the previous section, we explored proactive processes and tools that can be used to help avoid being surprised by issues and to aid in troubleshooting and resolution when they do arise. In this section, we will focus on what processes can be put in place to streamline response to issues once they’ve occurred.

Incident handling

Incident handling is a very broad topic, with a wide range of implementations and areas of expertise. It is beyond the scope of this document to cover even a fraction of them. The goal is to introduce the concept at a high-level, for further exploration and consideration.



Incident handling is defined as the business process by which incoming issues/tickets are triaged, assigned, investigated, and mitigated. Most organizations have an incident handling process, whether formalized or not. The advantage of a formalized process, with roles and responsibilities, troubleshooting parameters, and checklists, is to provide needed structure during difficult situations.

At a minimum, you should consider formalizing:

- Point of contact lists.
- Emergency change/revision control.
- Data gathering.
- Roll back policies and procedures.
- Escalation guidelines.

Point-of-contact lists

There should always be a clear and singular owner for individual application delivery components or areas of expertise. It is very common to have an on-call rotation per network, server, application, team, and so on., and for these rotations to hold true during business hours. A single point-of-contact for each problem domain makes communication much easier, and provides clear ownership and accountability. It also helps minimize chaos during incident handling.

It is also a good practice to have a list of backup names for each role and responsibility. Thought should also be given to vacation coverage and this list should be updated on a regular basis.

Emergency change/revision control

It is possible that the normal process for graduating changes into production is not realistic when troubleshooting an event real-time. A secondary process for migrating emergency changes made to production into the change/revision control process is a prudent measure, so that administrators can focus on troubleshooting measures, while easily capturing their modifications after everything is resolved.

Data gathering

The vast majority of the time, the same data sources will be used repeatedly, regardless of the nature of the event encountered. Prescribing a tailored list of data to gather at the onset of any issue can further minimize chaos by providing a clear sense of direction, while ensuring that critical data is captured in a time-sensitive manner. Time-based events are extremely difficult to analyze after the fact without the right supporting documentation. (See [Root-cause analysis \(RCA\)](#).)

The [Optimize the support experience](#) contains a comprehensive list of the information and supporting documentation needed when engaging F5 Technical Support, along with the circumstances under which each is required.



Roll back policy and procedure

For each maintenance period or upgrade, there should be a well-understood path back to a previous version, environment, or configuration. Ideally, this policy and process should be standard, and include clear criteria and decision points for whether to fall back or fix forward. If the decision is to fall back, there should be a standard process for doing so. If the decision is to fix forward, then there should be established escalation procedures to ensure the issue is resolved quickly. For more information, see Escalation Guidelines in the next section.

Escalation guidelines

Documenting the steps that should be taken before engaging F5 Technical Support for assistance, along with what conditions warrant immediate engagement of F5 Technical Support, can help minimize disruption and maximize responsiveness when it is most needed.

Designate a primary representative (“point person”), along with infrastructure and instructions for collaboration by the points-of-contact. This small step can dramatically improve communication and minimize confusion.

Root-cause analysis (RCA)

This section covers the steps you can take to ensure a successful investigation of your problem and may speed its resolution by F5 Technical Support. Although it is impossible to trace every problem back to its original (root) cause, there are certain steps you can take to maximize the chances of success.

Root-cause analysis (RCA) is the process of reviewing all available forensic and diagnostic information from a problem to determine the order of events that led to the failure, and to identify the original (root) event that triggered these downstream events. Determining the conditions that led to a problem may prevent it from recurring.

RCAs are very difficult to do, even under the best of circumstances. The more comprehensive the information gathering process is, the better the odds of success. It is your responsibility to ensure that you are capturing sufficient data should a RCA become necessary. The Optimize the Support Experience chapter contains a wealth of information on this subject. A lack of sufficient information or details can make an accurate and complete RCA difficult or impossible.

Gathering relevant information is useful when conducting a RCA, but at a minimum, it is desirable to have:

- A detailed description of the event.
- Date and time of occurrence(s).
- Any recent changes to the overall environment.
- Diagnostic and forensic data.

For more information, see [Optimize the support experience](#).



Proactive steps to aid future RCAs

Implement some form of change and revision control. Knowing what changed, when, and by whom, is critical to doing an effective RCA. The absence of this information is, by far, the most common reason RCAs are incomplete or not possible.

Invest in network monitoring/capturing tools. External information collection from the entire environment can be essential to correlation. Having multiple sources of similar information goes a long way to forming more concrete conclusions and can expose inaccurate or compromised data sources. Multiple data sources can be used to reinforce or refute each other.

Implement centralized logging

Sending log messages off-device into a central system can preserve historical data for much longer periods. It also enables correlation with other logging sources in the environment, and makes tampering with the information more difficult in the case of an intrusion.

Enable audit logging

The extent to which audit logging is implemented can be determined by operational requirements and industry standards, but should be considered required if change/revision control is not implemented.



Appendix C: Support Incident Report

Support Incident Report

F5 Technical Support may be able to resolve your support issues more quickly when provided with the data they need for troubleshooting. The worksheet below can help you prepare for opening a case.

Support contract details

- License number(s) of affected hardware:
- Your “Point of Contract” details:
- What alternative contacts are also available to work on the issue if you are not available?
- What hours are you available to work on the issues?
- Is remote access available?

Issue details

- What are the symptoms of the issue?
- What time did the issue first occur?
- How many has the issue recurred?
- What error output has been provided by the system?
- What are the steps to reproduce the issue?
- What changes have you made to the system before the issue first occurred?
- What step have you attempted to resolve the issue?
- Is this a new implementation?
- How many datacenters and devices are applicable to the configuration?
- Which devices are affected by the issue?
- Have you reviewed your uploaded qkview to BIG-IP iHealth? (Ensure that any qkviews uploaded to BIG-IP iHealth are linked to the support case.)



Which of these descriptions describe the impact of the issue on your site? (Choose one.)

- Site down: All network traffic has ceased, causing a critical impact to your business. Site at risk: Primary unit has failed resulting in no redundancy. Site is at risk of going down.
- Performance degraded: Network traffic is partially functional causing some applications to be unreachable.
- General assistance: Questions regarding configurations. Troubleshooting non-critical issue or request for product functionality that is not part of the current product feature set.

Opening a Support Case

See the following product-specific articles for details about the information you need to provide when opening a product-specific support case:

Table B.1: Articles to assist with assembling your support case

Product	AskF5 article
BIG-IP LTM, BIG-IP DNS, BIG-IP Link Controller, F5 MobileSafe™, F5 WebSafe	SOL135: Information required when opening a support case for BIG-IP LTM, AFM, GTM, Link Controller, PEM, F5 Mobile Safe, and F5 WebSafe.
BIG-IP WebAccelerator	SOL6705: Information required when opening a support case for BIG-IP WebAccelerator.
BIG-IP AAM	SOL14453: Information required when opening a support case for BIG-IP AAM.
BIG-IP APM / Edge Gateway	SOL11898: Information required when opening a support case for BIG-IP APM / Edge Gateway.
BIG-IP ASM	SOL6825: Information required when opening a support case for BIG-IP ASM.
BIG-IP PSM	SOL9360: Information required when opening a support case for BIG-IP PSM.
BIG-IP Analytics	SOL13066: Information required when opening a support case for BIG-IP Analytics.
BIG-IP AFM	SOL135: Information required when opening a support case for BIG-IP LTM, AFM, GTM, Link Controller, PEM, F5 Mobile Safe, and F5 WebSafe.
BIG-IP PEM	SOL135: Information required when opening a support case for BIG-IP LTM, AFM, GTM, Link Controller, PEM, F5 Mobile Safe, and F5 WebSafe.
Data Manager	SOL11537: Information required when opening a support case for Data Manager.
FirePass	SOL4274: Information required when opening a support case for FirePass.



Product	AskF5 article
WANJet	SOL6704: Information required when opening a support case for WANJet.
Enterprise Manager	SOL7569: Information required when opening a support case for Enterprise Manager.
ARX	SOL8244: Information required when opening a support case for ARX®.
Traffix SDC™	SOL14655: Information required when opening a support case for Traffix SDC.