F5 BIG-IQ Centralized Management: Monitoring and Reports

Version 5.4

Table of Contents

Health monitoring and alerts using SMTP and SNMP alerts....7
Health and event monitoring using SMTP and SNMP alerts.... 7
Alerts for managed devices and suggestions for troubleshooting....7
Specify an SMTP server to send email alerts....9
How do I set up BIG-IQ to work with SNMP?....10
Before you configure SNMP....10
Configuring SNMP agent for sending alerts....10
Configure Access and Traps for SNMP version 3 to send alerts....11
Configuring Access and Traps for SNMP version 1 and 2C to send alerts.... 12
Add email recipients for SMTP and SNMP alerts.... 12
How do I monitor SSL certificate expiration dates for my managed devices?.... 13
Set up alert conditions that triggers BIG-IQ to send a notification.... 13

Statistics Monitoring Overview.... 15
What analysis can I perform using collected statistics?....15
How do I get started managing statistics data?.... 15
What elements make up a statistics overview screen?....15
How do the time controls work?.... 16
How does the chart pane work?....17
How does the dimensions pane work?....18
What is different about a DNS statistics overview screen?.... 20

Configuring Statistics Collection....23
How do I start viewing BIG-IP device statistics from BIG-IQ?....23
Enabling statistics collection during device discovery.... 23
Enable statistics collection for devices.... 24
Manage the retention policy for your statistics data.... 25

Analyzing Statistics Data.... 27
Browse through your managed devices looking for high resource usage....27
Analyze application performance issues....28
Analyze load balancing issues....29
Troubleshoot DNS traffic issues....30

Managing Audit Logs.... 31
About audit logs.... 31
Actions and objects that generate audit log entries.... 31
Audit log entry properties....32
Viewing audit entry differences.... 33
Filtering entries in the audit log....33
Customizing the audit log display....35
Managing audit log archive settings....35
About archived audit logs....36
About audit logs in high-availability configurations....37
About the REST API audit log....37
Managing the REST API audit log....37

Access Reporting and Statistics..39

About Access and SWG reports 39

Setup requirements for Access and SWG reports 39

What data goes into Access reports for the All Devices option? 39

About upgrades affecting reports... 40

About the application dashboard... 40

View the Application Summary dashboard... 40

About application visibility... 40

About user visibility.. 40

Managing a specific user in Access reporting...41

Running Access reports...41

Getting the details that underlie an Access report 42

About the maximum number records for Access and SWG reports 43

Setting the timeframe for your Access or SWG report...43

Access report problems: causes and resolutions... 44

What can cause logging nodes to become unavailable? 44

Sessions... 44

Running Session reports...44

Stopping sessions on BIG-IP devices from Access... 45

Running Secure Web Gateway reports..45

About denied sessions.. 46

Viewing denied sessions...46

Getting the details that underlie an SWG report 46

About VDI reports...47

About network access reporting...47

View the network access summary..47

About network access performance...48

About network access reconnect.. 48

About network access errors...48

About network access usage... 49

About endpoint security check... 49

About endpoint software summary...49

About endpoint software details.. 50

Managing federation reports... 50

Running OAuth reports..50

Running SAML reports..51

Troubleshooting Access reporting..54

Overview: About troubleshooting Access reports...54

BIG-IP Application Visibility: How to configure the BIG-IP system.................................... 59

Overview: About the BIG-IP configuration for BIG-IQ application visibility.......................59

View the Application Summary dashboard.. 60

What is a basic configuration?... 60

What is an advanced configuration?.. 61

How much memory does application visibility need?...65

Application visibility troubleshooting commands.. 65

Managing Security Reports.. 67

About security reporting..67

Monitoring Active Firewall Policies..69

View active firewall policies.. 69

Active firewall policy rule properties.....69

Monitoring Firewall Rules.....71
About firewall rule monitoring.....71
Monitoring firewall rule statistics and hit counts.....71
Monitoring firewall rule compilation statistics.....72

Managing Firewall Rule Reports.....73
About firewall rule reports.....73
Creating firewall rule reports.....73
Deleting firewall rule reports.....74

Managing Firewall Packet Traces.....75
About firewall packet traces.....75
Create firewall packet traces.....75

Viewing Event Logs in Web Application Security.....77
About event log viewing.....77
View event logs and define filters and tags.....77
Use event log filters.....78
View and delete event log tags.....78

Determine DNS Sync Group Health.....79
How do I check my sync group health?.....79
Check DNS sync group health.....79
How do I set up an alert for DNS sync group issues?.....83

Viewing GSLB Objects.....85
View GSLB objects.....85
How do I manage permissions for DNS GSLB objects?.....85

Troubleshooting using iHealth.....87
What is iHealth?.....87
How do I get access to send QKView files for my managed devices to the F5 iHealth diagnostics server?.....87
Limit the number of simultaneous iHealth-related file transfers to and from BIG-IQ for my managed devices.....87
Upload a QKView file to the F5 iHealth server to troubleshoot potential issues... 87
Troubleshoot potential issues by viewing an iHealth device report.....88
Create a schedule to upload QKView files to the iHealth server.....88
Create an upgrade advisor report before you upgrade BIG-IP system 89

Legal Notices.....91
Legal notices.....91

Health monitoring and alerts using SMTP and SNMP alerts

Health and event monitoring using SMTP and SNMP alerts

You can use F5® BIG-IQ® Centralized Management to easily monitor the health of your managed devices, as well as BIG-IQ itself, using the following tools:

- Simple Mail Transfer Protocol - SMTP is a standard for email transmission used for monitoring and alerting you to the health of devices in your network.
- Simple Network Management Protocol - SNMP is an industry standard protocol for monitoring devices on IP networks. Once configured, the SNMP agent sends data collected from BIG-IQ Device to your third-party SNMP manager. BIG-IQ is compatible with SNMPv1, SNMPv2c, and SNMPv3.

After you configure SMTP and/or SNMP (which you typically do when you initially set up BIG-IQ), you can specify email recipients to receive alerts when certain events occur. These alerts are configurable; you can enable and disable them, and, for some alerts, you can set specific thresholds to prompt an alert.

Alerts for managed devices and suggestions for troubleshooting

You can specify these alerts to help you manage BIG-IP® devices from F5® BIG-IQ® Centralized Management.

Alert	Enable if you want to know when	Action (if applicable)
Certificate expiration	A certificate for a BIG-IP device is within a specific number of days of expiring.	
Certificate expired	A certificate for a BIG-IP device has expired.	Update the certificate so the BIG-IP device can continue to manage traffic. 1. Click **Configuration** > **LOCAL TRAFFIC** > **Certificate Management** > **Certificate & Keys**. 2. Click the name of the expired certificate. 3. Click the **Renew Certificate** button.
DNS Sync failed	A synchronization failed for the DNS synchronization group.	Investigate and resolve the issue, then synchronize the group. Some potential reasons for this error might be: A network error, a BIG-IP device in the DNS sync group is unavailable (down), and so forth.
Data Collection Device snapshot failed	A snapshot for a Data Collection Device failed.	Investigate and resolve the issue, then rerun the failed snapshot.
Device CPU above threshold	The CPU usage for a BIG-IP device is over a specified threshold.	Rebalance resources as needed.

Alert	Enable if you want to know when	Action (if applicable)
Device backup failed	A backup failed for a BIG-IP device.	Investigate and resolve the issue, then rerun the failed backup. Some potential reasons for this error might be: A network failure, not enough space for the backup, the device is unavailable (down), another BIG-IQ has discovered this device and is managing it, and so forth.
Device could not be assigned to a Data Collection device	The maximum number of devices (200) has been assigned to a single Data Collection Device.	If you want to assign more BIG-IP devices, you must add another Data Collection Device. **1.** Click **System** > **BIG-IQ DATA COLLECTION** > **BIG-IQ Data Collection Devices**. **2.** Click the **Add** button.
Device is low on memory	The BIG-IP device is low on memory.	Investigate and resolve the issue.
Device software version update is required	A managed BIG-IP device is running a software version that is not compatible with the BIG-IQ software version.	This could happen after you upgrade BIG-IQ. To manage this BIG-IP device from BIG-IQ, you must upgrade it to a compatible software version. For more information about that process, refer to the *F5 BIG-IQ Centralized Management : Device Management* guide.
Framework update required	The framework for a BIG-IP device is not compatible with BIG-IQ.	This could happen after you upgrade BIG-IQ or update a BIG-IP device to version 11.x. To manage the BIG-IP device from BIG-IQ, you must update its framework. **1.** Click **Devices** > **BIG-IP DEVICES**. **2.** Select the check box next to the device. **3.** Click the **More** button, and select **Update Framework**.
HA error	There is an issue with communication between the peer BIG-IQ systems in an high availability configuration.	Investigate and resolve the issue. Some potential reasons for this error might be: A network failure, the peer is unavailable (down), and so forth.
License expired	The license for a BIG-IP device has expired.	For a BIG-IP device managed from BIG-IQ, reactivate and reinstall its license. ***Note:*** *BIG-IQ does not send alerts for unmanaged BIG-IP devices. If you have licensed a BIG-IP device you are not managing from BIG-IQ, you'll have to monitor the expiration dates directly on the BIG-IP device itself.* **1.** Click **Devices** > **LICENSE MANAGEMENT** > **Licenses**. **2.** Click the name of the license. **3.** If the **License Status** doesn't display as `Active`, click the **Reactivate** button. **4.** Find the license assignment and click the **Refresh** button to reinstall the reactivated license.

Alert	Enable if you want to know when	Action (if applicable)
Managed Device Available	BIG-IQ successfully contacted a BIG-IP device.	
Managed Device Unavailable	BIG-IQ cannot reach a BIG-IP device.	Check the health and status of the BIG-IP device, and resolve the issue. Some potential reasons for this error might be: A network error, a BIG-IP device is offline for maintenance, another BIG-IQ has discovered this device and is managing it, and so forth.
Statistics Collection Agent update required	A BIG-IP device has an older version of the stats agent installed.	Update the stats agent for the BIG-IP device. **1.** Click **Devices** > **BIG-IP DEVICES**. **2.** Select the check box next to the device. **3.** Click the **More** button, and select **Update Stats Agent**.
Statics Collection did not happened when expected	BIG-IQ has exceeded the time configured for the frequency of statistics collection for a device. The default is 60 seconds	This could be caused by an expired license, communication issues, and so forth. To troubleshoot, take a look at the device. **1.** Click **Devices** > **BIG-IP DEVICES**. **2.** Click the name of the device. **3.** Look into any reported issues.
Used disk space is above threshold for a DCD	The disk space on a DCD is running out.	Take a look at your resources and adjust as needed.
Used disk space is above threshold for a device	The disk space for a device is over a specified threshold.	Check the BIG-IP device for non-critical files, such as old `tcpdump`, `qkview`, or `core` files. If you are uncertain about files to remove, contact *F5 Technical Support* for assistance.

Specify an SMTP server to send email alerts

You specify an SMTP server so F5® BIG-IQ® Centralized Management can send email to alert specified people when a certain condition happens, such as when an SSL certificate is about to expire.

1. At the top of the screen, click **System**.
2. On the left, click **SMTP Configuration**.
3. On the SMTP Configuration screen, if there is no mail server set up, click the **Add** button.
4. In the **Name** field, type a name for this SMTP configuration.
5. In the **SMTP Server Host** and **SMTP Server Port** fields, type the SMTP server and TCP port.

   By default, SMTP uses TCP 25.
6. In the **From Email Address** field, type the email address from which to send the alert email.
7. From the **Encryption** list, select the type of encryption to use for the email.
8. To require a user name and password, from the **Use Auth** list, select **Yes**, and type the required user name and password.

9. To verify that you can reach the server you configured, click the **Test Connection** button.
10. Click the **Save & Close** button at the bottom of the screen.

You can now specify email recipients and set up the alert conditions that prompt BIG-IQ to send an email when a certain event happens on a managed device.

How do I set up BIG-IQ to work with SNMP?

Simple Network Management Protocol (*SNMP*) is an Internet-standard protocol for collecting and organizing information about managed devices on IP networks. You can set up BIG-IQ® to work with SNMP so you can receive alerts when certain things happen on a managed device.

To set up BIG-IQ to work with SNMP, you must:

1. Set up the SNMP Agent
2. Configure SNMP Access
3. Specify settings for the SNMP Trap

Before you configure SNMP

Gather the following information before you start your SNMP configuration.

CONFIGURATIO N COMPONENT	CONSIDERATIONS	FOR MY CONFIGURATION
SNMP administrator contact information	Find out or decide who is responsible for SNMP administration. The contact information is a MIB-II simple string variable.	
Machine location	Find out the location of the BIG-IQ system. The location is a MIB-II simple string variable.	
BIG-IQ client allow list	Gather the IP or network addresses (with netmasks) of the SNMP managers from which the SNMP agent will accept requests.	
Access	Find the OID for the top-most node of the SNMP tree to provide access to.	
Community	Get the v1 and v2c communities and the IP addresses of the SNMP managers you want to grant access to.	
Users	Get the v3 users you want to grant access to SNMP data, along with the privacy protocols and passwords, Community, Destination, and Port.	

Configuring SNMP agent for sending alerts

This screen displays specified user addresses allowed to access your 3rd-party SNMP Manager BIG-IQ through the SNMP Agent. An agent can communicate with multiple managers, so you can configure BIG-IQ to support communications with one management station using the SNMP version1 protocol, one using the SNMP version 2C protocol, and another using SMNP version 3.

1. At the top of the screen, click **System**.
2. On the left, click .
3. At the top of the screen, click the **Download MIB** button to download the F5-required MIBs.
4. At the top of the screen, click **Edit**.
5. Edit the **Contact Information** and **Machine Location** fields to reflect your SNMP agent settings and click the **Save & Close** button at the bottom of the screen.
6. Click the **Save & Close** button at the bottom of the screen to save your changes.
7. For the **SNMP Access - Client Allowed List** setting, click the **Add** button.
8. In the **Addresses/Networks** and **Mask** fields, type the IP address and networks and the netmask (if applicable) that the SNMP manager is allowed to access.
9. To add another address, click the plus (+) sign.
10. At the bottom of the screen, click the **Save & Close** button.

You can now configure SNMP access and SNMP traps.

Configure Access and Traps for SNMP version 3 to send alerts

After you configure the SNMP agent, you can configure SNMP access and SNMP traps.

You configure SNMP access to allow the SNMP agent to accept requests from specific SNMP managers.

1. At the top of the screen, click **System**.
2. On the left, click **LOCAL HOST SETTINGS** > **SNMP Configuration** > **SNMP Access (v3)**.
3. Click the **Add** button at the upper right of the screen.
4. In the **Name** and **User Name** fields, type a name for this SNMP access and the user name.
5. If you want to specify the authentication protocol for SNMP traps, from the **Type** list, select an option.
   - **MD5** specifies digest algorithm.
   - **SHA** specifies secure hash algorithm.
6. If you selected an authentication protocol, in the **Password** and **Confirm Password** fields, type and confirm the password for access.

   The password must be between 8 and 32 characters, include alphabetic, numeric, and special characters, but no control characters.
7. If you want to encrypt the SNMP traps, from the **Protocol** list, select an option.
   - **AES** specifies Advanced Encryption Standard
   - **DES** specifies Data Encryption Standard
8. If you selected a privacy protocol, in the **Password** and **Confirm Password** fields, type the password to use for authentication.

   Alternatively, you can select the **Use Authentication Password** check box to use the authentication password.
9. In the **OID** field, type the object identifier (OID) you want to associate with this user.
10. From the **Access** list, select an option:
    - **Read Only** - This user can only view the MIB.
    - **Read/Write** - This user can view and modify the MIB.

    The most secure access level or type takes precedence when there is a conflict. When you set the access level to read/write, and an individual data object has a read-only access type, access to the object remains read-only.
11. Click the **Save & Close** button at the bottom of the screen to save your changes.
12. On the left, click **SNMP Traps**.

13. In the **Name** field, type a name for this SNMP trap.
14. From the **Version** list, select **V3**.
15. In the **Destination** and **Port** fields, type the IP address and the port for this trap destination.
16. For the **Security Level** setting, select an option. **Auth, No Privacy** processes SNMP messages using authentication, but no encryption. **Auth and Privacy** processes SNMP messages using authentication and encryption.
17. For the **Security Name** setting, specify the user name you want to use to handle SNMP version 3 traps.
18. For the **Engine ID** setting, specify the unique identifier (snmpEngineID) of the remote SNMP protocol engine.
19. In the **Password** and **Confirm Password** fields, type and confirm the password for the protocol.
20. Click the **Save & Close** button at the bottom of the screen to save your changes.

You can now specify email recipients for alerts.

Configuring Access and Traps for SNMP version 1 and 2C to send alerts

After you configure the SNMP agent, you can configure SNMP access and SNMP traps.

You configure SNMP access to allow the SNMP agent to accept requests from specific SNMP managers.

1. At the top of the screen, click **System**.
2. On the left, **LOCAL HOST SETTINGS** > **SNMP Configuration** > **SNMP Access (V1, V2C)**
3. At the top left of the screen, click the **Add** button.
4. In the **Name** field, type the SNMP manager's user name.
5. From the **Type** list, select the format for the IP address.
6. In the **Community** field, type the community string (password) for access to the MIB.
7. From the **Source** list, select a source or select **Specify** and type the source address for access to the MIB.
8. In the **OID** field, type the object identifier (OID) you want to associate with this user.
9. From the **Access** list, select an option:

    - **Read Only** - This user can only view the MIB.
    - **Read/Write** - This user can view and modify the MIB.

    The most secure access level or type takes precedence when there is a conflict. When you set the access level to read/write, and an individual data object has a read-only access type, access to the object remains read-only.
10. Click the **Save & Close** button at the bottom of the screen to save your changes.
11. On the left, click **SNMP Traps**.
12. At the top left of the screen, click the **Add** button.
13. In the **Name** field, type a name for this SNMP trap.
14. In the **Community**, **Destination**, and **Port** fields, type, respectively, the community name, IP address, and port for the trap destination.
15. At the bottom of the screen, click the **Save & Close** button.

You can now specify email recipients for alerts.

Add email recipients for SMTP and SNMP alerts

After you configure SMTP and/or SNMP, you can add email recipients.

Email recipients you add will get alert notifications when specified events happen on BIG-IQ or your managed devices

1. At the top of the screen, click **System**.
2. On the left, click **LOCAL HOST SETTINGS** > **Email Notification Recipients**.
3. At the top left of the screen, click the **Add** button.
4. In the **Name** the **Email** address fields, type the name and email address of the person you want to receive an alert.
5. In the **Description** field, you can type an optional description to help identify this user.
6. Select the check box next to each type of notification you want this user to receive an email about.
7. To add another email recipient, click +.
8. Click the **Save & Close** button at the bottom of the screen to save your changes.

You can now configure the alert settings that trigger BIG-IQ to send an email to the specified recipients.

How do I monitor SSL certificate expiration dates for my managed devices?

When you manage BIG-IP® devices that load balance SSL traffic, you must monitor their SSL traffic.

BIG-IQ® imports the certificates for every managed BIG-IP device you discover. This makes it easy to monitor the expiration dates all of your devices' SSL certificates from one location.

You can also:

- Set up alerts to let you know when a certain certificate is about to expire within a specified number of days.
- Download the data to a CSV file for reporting purposes.

Set up alert conditions that triggers BIG-IQ to send a notification

After you set up the SNMP and/or SMTP on F5 ®BIG-IQ® Centralized Management, you can select the alerts that prompt BIG-IQ to send an email to the people you specified.

1. At the top of the screen, click **Monitoring**.
2. On the left, click **ALERTS & NOTIFICATIONS.**
3. At the top of the screen, click the **Settings** button.
4. Select the **Enabled** check box next to each alert you want to receive and, if applicable, specify the **Threshold**.

   Only SNMP events specified as **Yes** are available for SNMP alerts. BIG-IQ uses SMTP for all other event types.
5. Click the **Save & Close** button at the bottom of the screen.

Statistics Monitoring Overview

What analysis can I perform using collected statistics?

You can use the statistics collected by F5® BIG-IQ® Centralized Management to visually analyze the performance of Local Traffic objects, device traffic, DNS traffic, and overall system statistics. The statistics are displayed in graphical charts and tables that you can drill down into for more specific details. You might want to track network performance on a device, or memory and CPU utilization; or you might want to compare the performance on two devices or a group of devices. You can focus the statistics in the charts on different categories such as virtual servers, pools, pool members, or DNS traffic.

How do I get started managing statistics data?

You can monitor statistics data generated by the devices you manage. You can monitor the performance of your BIG-IQ® devices as well, but that works differently and is discussed in the online help. There are a few things you need to do before you can start monitoring the statistics data generated by your managed devices.

- You need to install, configure, and discover a data collection device (DCD). The DCD stores the data from your devices, and routes the date to your BIG-IQ device. Refer to *Planning and Implementing a Centralized Management Deployment* for details.
- You need to enable statistics collection for the devices you want to monitor. There a couple of ways to do that. Refer to *Enabling Statistics Collection* for details.

Once you have your system set up and you are receiving statistics, you should take a minute or two to understand how the user interface works. The interface is set up so that statistics from Device, DNS, and Local Traffic use a common set of tools to manage how you access and manage your data. Once you understand how this common interface works, you should be ready to go.

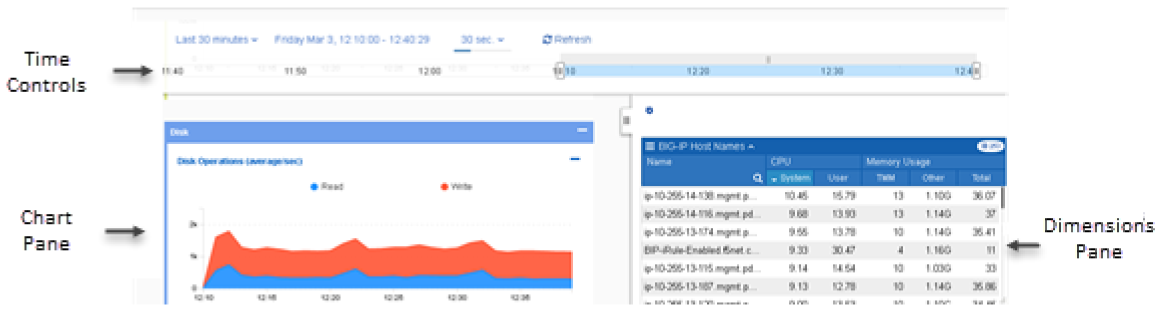
Important: *Statistics for the Access component use a slightly different user interface. For details on monitoring these statistics, refer to Access Reporting and Statistics.*

Important: *Statistics for this BIG-IQ device also use a different user interface. For details on monitoring these statistics, go to* ***System*** *>* ***THIS DEVICE*** *>* ***Statistics****, or* ***System*** *>* ***THIS DEVICE*** *>* ***BIG-IQ Metrics*** *and refer to the online help.*

What elements make up a statistics overview screen?

This figure shows a typical statistics overview screen. The three parts of the statistics overview screens work together so you can fine-tune the statistics display. To view a screen similar to this, click **Monitoring** > **DASHBOARDS** > **Device** > **Health**. However, until you configure statistics collection, there won't be any data.

Note: *The Overview screen for DNS has a few extra controls. For details, see What is different about the DNS Overview screen?.*



Name	CPU System	User	Memory Usage TMM	Other	Total
ip-10-255-14-138.mgmt.p...	10.46	15.79	13	1.10G	36.07
ip-10-255-14-116.mgmt.pd...	9.68	13.93	13	1.14G	37
ip-10-255-13-174.mgmt.p...	9.56	13.78	10	1.14G	35.41
BIP-iRule-Enabled.f5net.c...	9.33	30.47	4	1.16G	11
ip-10-255-13-115.mgmt.pd...	9.14	14.54	10	1.03G	33
ip-10-255-13-187.mgmt.p...	9.13	12.78	10	1.14G	35.86

Figure 1: Typical statistics overview screen

The table defines key elements of this screen.

User interface area	What does this part of the screen do?
Time Controls	Adjusts the time window for which statistics are displayed. For details on how these controls work, see *How do the time controls work?*.
Chart Pane	Displays a series of charts that plot the collected statistics. For details on how to manipulate these charts, see *How does the chart pane work?*.
Dimensions Pane	Determines the objects for which you display statistics. For details on how the controls on this pane work, see *How does the dimensions pane work?*.

How do the time controls work?

This figure shows a close up of the time controls on a typical overview screen. To view a screen similar to this, click **Monitoring** > **DASHBOARDS** > **Device** > **Health**.The four time controls work together to give you control of the specific time period for which you wan to see statistics.

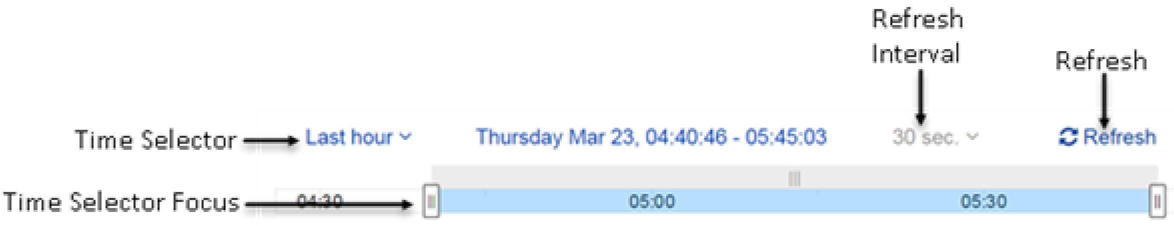


Figure 2: Overview screen time control detail

Key elements of this screen are defined in the table.

User interface control	What does this control do?
Time Selector	Use this control to specify the length of time for which you want to view statistics data. When you first start looking at statistics, only the **All** option is available. Then as you gather additional data, additional time period options become available. Data is displayed from the instant the last refresh occurred, back to time interval you specify. For example, if the last refresh occurred at 11:00, and the Time Selector is set to 30 minutes, the charts display data from 10:30 to 11:00.
Time Selector Focus	Use this control to focus on a specific window of time within the currently selected time period. Use the sliders at either end of this control to define the time segment you want to examine. The time segment you select here is indicated along the lower horizontal axis of the chart pane to provide a

User interface control	What does this control do?
	reference. For example, if the last refresh occurred at 11:00, and the Time Selector is set to 30 minutes, you could use the sliders to look at the period from 10:45 to 10:50. When you adjust the sliders, the time markers along the bottom of each chart axis update to indicate your selection. Also, note that you can adjust both ends of this control. If you adjust the right side of the control, the auto refresh stops, effectively freezing the display so you can focus on a particular data point. ***Tip:*** *Alternatively, you can click on the chart axis to specify the focus. Click on a point in the axis and drag in the direction that you want to view. As you drag, a highlighted window shows what you have selected for the time selector focus, and a small magnifying glass icon appears. When you have the time selector focus you want, click the magnifying glass.*
Refresh Interval	Use this control to specify how frequently the data on this page is refreshed.
Refresh	Use this control to trigger an immediate refresh of the data on this screen.

How does the chart pane work?

This figure shows a closer look at the elements that make up the chart pane on a typical Overview screen. To view a screen similar to this, click **Monitoring** > **DASHBOARDS** > **Device** > **Health**. You can re-order the charts by dragging and dropping them into place.

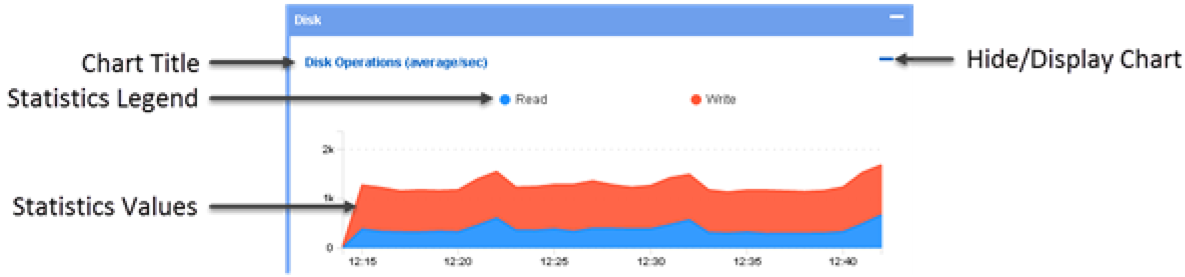


Figure 3: Overview screen, chart pane detail

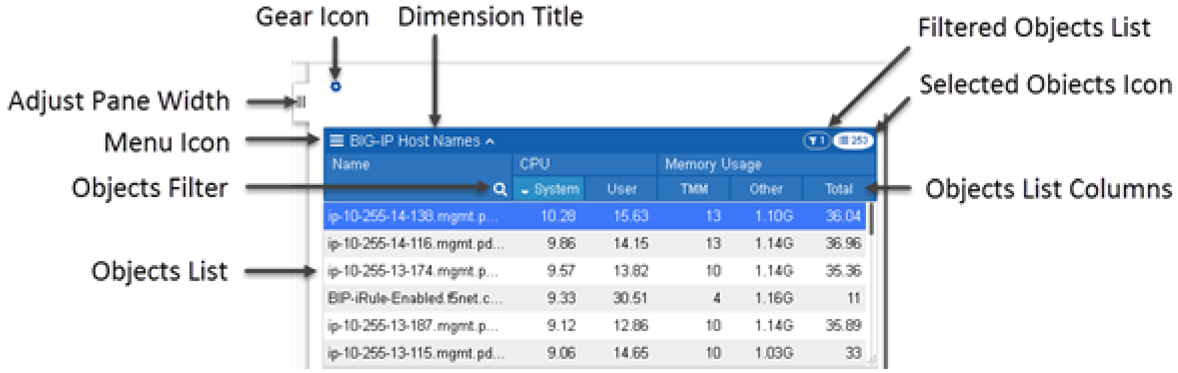
Key elements of this screen are defined in the table.

User interface control	What does this control do?
Chart Title	Each chart displays a title that identifies the statistic that plots on that chart. Each title includes the units of measure that apply to these plots.
Statistics Legend	These colored dots identify the specific plots displayed on the chart. When you move your cursor over a chart, the value of each plot displays adjacent to these dots. If there is a multiplier applied to a value, it displays as well. For example, if you hover over one of the New Connections plots and the value `31.9k` displays, it means that there were an average of 31,900 connections per second at that point in time.
Statistics Values	These plots display the value of the statistics collected for the selected time period. Data is aggregated for the objects or devices that are currently selected. Initially, the selection is all of the managed objects or devices, but you can

User interface control	What does this control do?
	use the dimensions pane to change the selection. If you select one device, the charts shows statistics for just that device. If you select two devices, the charts plot aggregated statistics for those devices. If you then select just one device, and five virtual servers, the charts plot aggregated statistics for the five virtual servers and the single device. For more information on using the dimensions pane refer to *How does the dimensions pane work?*
Hide/Display Chart	Use this control to hide or display a chart. When you hide a chart, the chart title remains. If you create a comparison chart, an additional control appears that you can use to delete that chart.

How does the dimensions pane work?

In the BIG-IQ® user interface, a dimension is a statistical category (for example BIG-IP® host name or iRule event types). Each dimension is broken up into sub-categories that you can view when you expand the dimensions pane to display your statistical data as a table. The other primary use for the controls in the dimensions pane is to filter the objects for which statistics are displayed in the chart window. To view a screen similar to the following illustration, click **Monitoring** > **DASHBOARDS** > **Device** > **Health** > , and then click the down arrow on the BIG-IP Host Names dimension. After you expand a dimension, you can select individual objects, or multiple objects, or create a comparison graph that displays statistics for selected objects. The figure shows the key elements that make up the dimensions pane on a typical Overview screen. You can re-order the dimensions by dragging and dropping them into place.



Name	CPU		Memory Usage		
	System	User	TMM	Other	Total
ip-10-255-14-138.mgmt.p...	10.28	15.63	13	1.10G	36.04
ip-10-255-14-116.mgmt.pd...	9.86	14.15	13	1.14G	36.96
ip-10-255-13-174.mgmt.p...	9.57	13.82	10	1.14G	35.36
BIP-iRule-Enabled.f5net.c...	9.33	30.51	4	1.16G	11
ip-10-255-13-187.mgmt.p...	9.12	12.86	10	1.14G	35.89
ip-10-255-13-115.mgmt.pd...	9.06	14.65	10	1.03G	33

Figure 4: Overview screen dimensions pane detail

Key elements of this screen are defined in the table. Except for the name of each dimension and the pane width adjustment, these controls display only when you expand a dimension to display all of its members.

User interface control	What does this control do?
Adjust Pane Width	With this tab, you can adjust the width of the chart and dimensions panes. To adjust the dimensions pane width, click this tab and drag the pane to the width you want. To extend the dimensions pane to full screen, single click this tab.
Menu Icon	When you click the menu icon, you can choose between several options that you can use to change what is displayed in the Dimensions pane. • **Sort by** lists the columns defined for the selected object. You can choose which column you want to sort the listed objects by.

User interface control	What does this control do?
	• **Columns** lists the available columns that can be displayed for the selected object. You can choose which columns you want to display. For a list of what each column in the dimension pane specifies, see Dimension Pane Columns. ***Note:*** *You can also sort a dimension or specify which columns display by right-clicking the column header.* If you select one or more objects for a dimension, you can choose two additional options: • If you choose **Add Comparison Chart**, you can create a graph that plots values for two or more selected metrics. You can create multiple comparison charts and for each comparison chart, you change the metric that is being compared. • If you choose **Clear Selection**, you choose which objects you want to de-select.
Objects Filter	Click the magnifying glass to open a filter control. To filter the list of objects that display in the Objects List, type the name you want to find and click the magnifying glass again. Note that the filter is a prefix match (it starts with the first character of the object name), and the match is case-sensitive.
Objects List	The first 100 objects that meet the filter criteria display here. To display an object not in the top 100, you can change your filter criteria or sort order. Objects selected in the objects list, control the data that plots in the charts. That is: • When you select just one object, the data plotted on the charts is only for that object. • If you select additional objects, the data that plots is the aggregate for those selected objects. • When no objects are selected, the data that plots is the aggregate for all objects in the dimension. ***Note:*** *If you select two or more objects in this list, you can create a comparison chart that plots values for a selected parameter.*
Objects List Columns	The default number of columns that display depends on the type of dimension. You can also change which columns display using the menu icon. You can sort the entries in a dimension by clicking an individual column title. .
Dimension Title	The title of the dimension displays here adjacent to an up arrow/down arrow toggle. This toggle collapses and expands the list of objects of this dimension type for the devices you are currently managing.
Gear Icon	The gear icon provides several options that you can use to change how the objects you have selected in the Dimensions panel display. • You can use **Clear Filters**to de-select all of the objects for the selected dimension. • You can use **Reset Layout** to undo any custom sorting you have applied and reset the selected dimension to the default layout.

User interface control	What does this control do?
	• You can use **Sort Selected** to resort the list of objects for the selected dimension. With this filter applied, the objects you have selected move to the top of the column. Any type of sort you use to reorder this dimension change the sort order for the remaining objects, but the selected objects stay at the top of the list.
Selected Objects Icon	This icon displays the number of objects in this dimension that match the current filter settings. Note that the objects you select in one dimension impact the number of objects in the other dimensions. As an example, consider a BIG-IQ managing 20 BIG-IP devices that each have 100 virtual servers. Initially, on the Virtual Servers overview screen, the selected objects icon in the BIG-IP Host Names dimension reads 20, and the selected objects icon on the Virtual Servers dimension reads 2000. If you select one BIG-IP device, the icon for virtual servers changes to 100. On the other hand, if you select one of the virtual servers, the icon for BIG-IP devices would change to 1 (unless that virtual server happens to reside on more than one device).
Filtered Objects Icon	This icon displays the number of objects you have selected in this dimension. You can also click this icon to de-select all objects in this dimension.

Comparison Charts

Comparison charts allow you to plot data values for selected items in a new chart. When you initially create a comparison chart, you select the statistical metric that you want to compare. When the comparison chart displays, the title for the new chart displays which items are selected for comparison, along with the metric being compared, followed by a down arrow icon. You can click that down arrow if you want to change the comparison metric for the selected objects. To compare additional items, you can create additional comparison charts by again selecting multiple items, right clicking and choosing Create Comparison Chart, and selecting the statistical metric you want to compare.

What is different about a DNS statistics overview screen?

This figure shows a typical DNS statistics overview screen. To view a screen similar to this, click **Monitoring** > **DASHBOARDS** > **DNS** > **Overview**. Until you configure statistics collection, there won't be any data. You can use the time controls to focus on a time period of interest, similar to other overview screens. However, there are unique elements on this screen that provide you with a quick overview summarizing the DNS traffic performance on your managed devices.

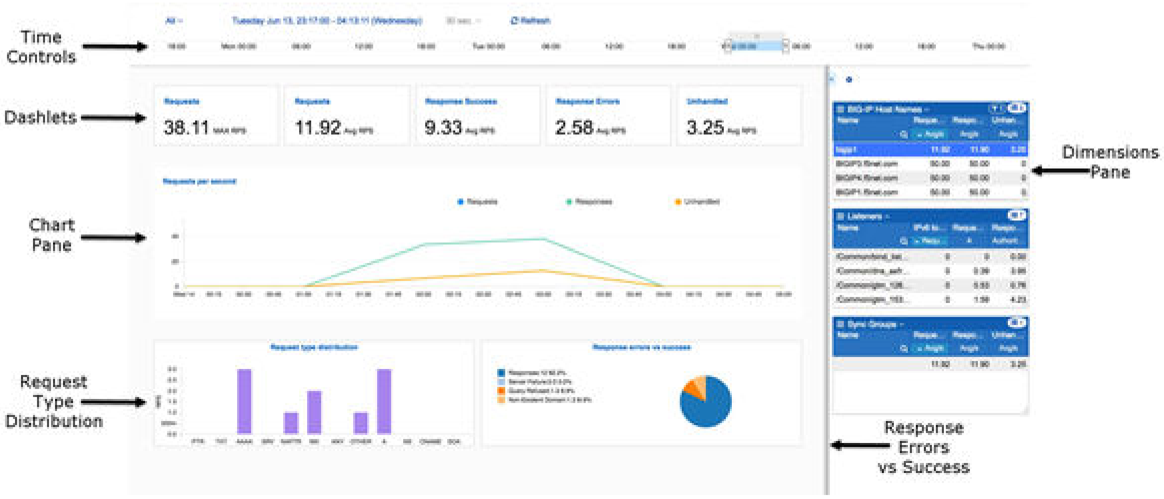


Figure 5: Typical DNS Sync group statistics overview screen

Key elements of this screen are defined in the table.

User interface control	What does this part of the screen do?
Time Controls	Adjusts the time window for which statistics are displayed. For details on how these controls work, see *How do the time controls work?*
Dashlets	These small windows serve similarly to the gauges on a dashboard, providing a current performance readout for key performance statistics.
Chart Pane	Displays a series of charts that plot the collected statistics. For details on how to manipulate these charts, see *How does the chart pane work?*
Request Type Distribution	This chart graphs the types of request that are currently being processed by this DNS sync group.
Response Errors vs Success	This chart graphs the DNS sync group's success rate in processing requests relative to the number of requests that result in errors.
Dimensions Pane	Determines the objects for which you display statistics. For details on how the controls on this pane work, see *How does the dimensions pane work?*

Configuring Statistics Collection

How do I start viewing BIG-IP device statistics from BIG-IQ?

To start viewing statistics for a BIG-IP® device, you must enable statistics collection for that device. You can do that either during or after adding the device to the BIG-IP Devices inventory list on the BIG-IQ® system. You also need to install, configure, and add a data collection device before you can view device statistics.

Enabling statistics collection during device discovery

Before you can enable statistics for BIG-IP® devices:

- There must be a BIG-IQ® data collection device configured for the BIG-IQ device.
- The BIG-IP device must be located in your network and running a compatible software version. Refer to *https://support.f5.com/kb/en-us/solutions/public/14000/500/sol14592.html* for more information.
- Port 22 and 443 must be open to the BIG-IQ management address, or any alternative IP address used to add the BIG-IP device to the BIG-IQ inventory. These ports and the management IP address are open by default on BIG-IQ.

If you are running BIG-IP version 11.5.1 up to version 11.6.0, you might need `root` user credentials to discover and add the device to the BIG-IP devices inventory. You don't need `root` user credentials for BIG-IP devices running versions 11.6.1 - 12.x.

Note: *A BIG-IP device running versions 10.2.0 - 11.5.0 is considered a legacy device and cannot be discovered from BIG-IQ version 5.2. If you were managing a legacy device in previous version of BIG-IQ and upgraded to version 5.2, the legacy device displays as impaired with a yellow triangle next to it in the BIG-IP Devices inventory. To manage statistics for it, you must upgrade it to version 11.5.1 or later. For instructions, refer to the section titled, Upgrading a Legacy Device.*

One way to enable statistics collection for BIG-IP devices is to do it when you add those devices to the BIG-IQ system inventory. Adding devices to the inventory is referred to as *device discovery*. If the devices you want to enable have already been discovered, refer to *Enabling collection after device discovery*.

Note: *The ADC component is automatically included (first) any time you discover or import services for a device.*

Note: *You do not need to discover and import a device's configuration to collect and view statistics for it. You just need to establish trust between your BIG-IQ and the device. If you do not discover and import the device configuration, the virtual servers, pool, pool members, and iRules will be visible in the statistics dimension panes, but these objects will not appear in the configuration page for those objects. Also, you will not be able to manage these objects in BIG-IQ. If you decide you want to manage these objects, you can discover and import the BIG-IP device's configuration later without interrupting statistics collection.*

1. At the top of the screen, click **Devices**.
2. Click the **Add Device** button.
3. In the **IP Address** field, type the IPv4 or IPv6 address of the device.
4. In the **User Name** and **Password** fields, type the user name and password for the device.
5. If this device is part of a DSC pair, for the **Cluster Display Name** setting, specify how to handle it:

- For an existing DSC pair, select **Use Existing** from the list, and then select the name of your DSC group from the next list.
- To create a new DSC pair, select **Create New** from the list, and type a name in the field.

For BIG-IQ to properly associate the two devices in the same DSC group, the **Cluster Display Name** must be the same for both members in a group.

There can be only two members in a DSC group.

6. If this device is configured in a DSC pair, for the **Deployment Settings**, specify how to handle it:
   - **Initiate BIG-IP DSC sync when deploying configuration changes (Recommended)**: Select this option if this device is part of a DSC pair and you want this device to automatically synchronize configuration changes with the other member in the DSC group.
   - **Ignore BIG-IP DSC sync when deploying configuration changes**: Select this option if you want to manually synchronize configurations changes between the two members in the DSC group.
7. Click the **Add** button at the bottom of the screen.
   The BIG-IQ system opens communication to the BIG-IP device, and checks the BIG-IP device framework.

   ***Note:** The BIG-IQ system can properly manage a BIG-IP device only if the BIG-IP device is running a compatible version of the REST framework.*
8. If a framework upgrade is required, in the popup window, in the **Root User Name** and **Root Password** fields, type the root user name and password for the BIG-IP device, and click **Continue**.
9. If in addition to basic management tasks (like software upgrades, license management, and UCS backups) you also want to centrally manage this device's configurations for licensed services, select the check box next to each service you want to discover.

   You can also select these service configuration after you add the BIG-IP device to the inventory.
10. To enable statistics collection for this BIG-IP device, under Statistics monitoring, select the check box next to each service you want to collect statistics for, and then click **Continue**.

    ***Note:** If you want to enable statistics collection without managing any services, just clear the check boxes for all services.*
11. Click the **Add** button at the bottom of the screen.

Enable statistics collection for devices

Before you can enable statistics collection for a BIG-IP® device using this method:

- The device must already be in the BIG-IQ system inventory.
- There must be a BIG-IQ data collection device configured for the BIG-IQ device.

Generally, if you want to collect statistics for a BIG-IP device, you enable statistics collection when you discover it. But you can enable or disable statistics collection for a device any time it is convenient for you.

1. At the top of the screen, click **Devices**.
2. Click the name of the device you want to enable statistics collection for.
3. On the left, click **Statistics Collection**.
4. To begin statistics collection, for **Collect Statistics Data**, select **Enabled**.
5. For **Modules/Services**, click the check box for the types of statistics you want to collect.
6. For **Frequency**, next to **Collect every**, select the interval at which you want to collect statistics from this device.

After you enable statistics collection for a device, data for that device begins aggregating along with any other devices for which you are collecting data. Two buttons (**View Health Statistics**, and **View Traffic**

Statistics) are added to the properties page for enabled devices. Clicking either of these takes you directly to the overview page for the statistics type you clicked.

Manage the retention policy for your statistics data

Before you can set the statistics retention policy, you must have added a data collection device.

You can manage the settings that determine how your statistics data is retained. The highest quality data is the raw data, (data that has not been averaged), but that consumes a lot of disk space, so you need to consider your needs in choosing your data retention settings. When you choose how much raw data to retain, you need to consider how much disk space you have available. The controls on this screen are simple to set up, but understanding how they work takes a bit of explanation.

The fields on the Statistics Retention Policy screen all work in similar fashion. One way to understand how these fields work is to think of your data storage space as a set of containers. The values you specify on this screen determine how much storage space each container consumes. Because data is saved for the time periods you specify, the longer the time period that you specify, the more space you consume. The disk storage that is consumed depends on several factors.

- The number of BIG-IP® devices you manage
- The number of objects on the BIG-IP devices you manage (for example, virtual servers, pools, pool members, and iRules®)
- The frequency of statistics collection
- The data retention policy
- The data replication policy

There are three key concepts to understand about how the retention policy works.

How long is data in each container retained?	Data is retained in each container for the time period you specify. When the specified level is reached, the oldest chunk of data is deleted. For example, if you specify a raw data value of 48 hours, then when 48 hours of raw data accumulate, the next hour of incoming raw data causes the oldest hour to be deleted.
When does data from one container pass on to the next?	Data passes from one container to the next in increments that are the size of the next (larger) container. That is, every 60 minutes, the last 60 minutes of raw data is aggregated into a data set and passed to the **Hour(s)** container. Every 24 hours, the last 24 hours of hourly data is aggregated into a data set and passed to the **Day(s)** container, and so on for the **Month(s)** container.
What about limits?	**Limit Max Storage to** specifies the percentage of total disk space that you want data to consume on the data collection devices in your cluster. If more disk space is consumed than the percentage you specified, BIG-IQ takes two actions: **1.** New statistical data is not accepted until the available disk space complies with the **Limit max storage to** setting.

	2. Statistical data not required to calculate the next higher time layer is removed (for example, you need 60 minutes of raw data to aggregate to the Hours level). Data is removed starting with the raw data container, then the hourly data container, then the daily time container. This process stops when storage consumption is below the **Limit max storage to** setting. The BIG-IQ takes this action to prevent data corruption when storage is completely exhausted.

1. At the top of the screen, click **System**, and then, on the left, click **BIG-IQ DATA COLLECTION** and select **BIG-IQ Data Collection Cluster**.
    - Under Summary, you can view information detailing how much data is stored, as well as how the data is stored.
    - Under Configuration, you can access the screens that control DCD cluster performance.
2. On the left, click **Configuration** > **Statistics Data Collection**.
   The Statistics Collection Status screen displays the percentage of available disk space currently consumed by statistics data for each container.
3. To change the retention settings for your statistics data, click **Configure**.
   The Statistics Retention Policy screen opens.
4. In the **Keep real-time (raw) data up to** field, type the number of hours of raw data to retain.

   You must specify a minimum of 1 hour, so that there is sufficient data to average and create a data point for the **Keep hourly data up to** container.
5. In the **Keep hourly data up to** field, type the number of hourly data points to retain.

   You must specify a minimum of 24 hours, so that there is sufficient data to average and create a data point for the **Keep daily data up to** container.
6. In the **Keep daily data up to** field, type the number of daily data points to retain.

   You must specify a minimum of 31 days, so that there is sufficient data to average and create a data point for the **Keep monthly data up to** container.
7. In the **Keep monthly data up to** field, type the number of monthly data points to retain.

   Once the specified number of months passes, the oldest monthly data set is deleted.
8. In the **Limit max storage to** field, type the percentage of disk space that you want collected data to consume before the oldest monthly data set is deleted.
9. Expand Advanced Settings, and then select the **Enable Replicas** check box.

   Replicas are copies of a data set that are available to the DCD cluster when one or more devices within that cluster become unavailable. By default, data replication for statistics is not enabled. Disabling replication reduces the amount of disk space required for data retention. However, this provides no protection from data corruption that can occur when you remove a data collection device. You should enable replicas to provide this protection.
10. When you are satisfied with the values specified for data retention, click **Save & Close**.

Analyzing Statistics Data

Browse through your managed devices looking for high resource usage

Before you can analyze BIG-IP® device performance data:

- There must be a BIG-IQ data collection device configured for the BIG-IQ® system that manages your BIG-IP devices.
- You must have discovered the BIG-IP devices that you want to analyze, and statistics collection must be enabled for those devices.
- It is also a good idea, though not a requirement, to define the retention policy for the statistics data you are collecting.

You can use the Device Health overview screen to review the resource usage for your BIG-IP devices.

1. At the top of the screen, click **Monitoring**.
2. On the left, click **DASHBOARDS** > **Device** > **Health**.
   The Device Health overview screen opens.
3. On the Device Health overview screen, adjust the dimensions pane so that it fills up at least half of the screen.
4. In the dimensions pane, click the down arrow on the BIG-IP Host Names dimension to expand the list of BIG-IP devices.
5. In the CPU column click the **System** heading to sort the list of BIG-IP devices by CPU usage.
6. If you find a device that is consuming a high level of CPU cycles, select it.
   The chart pane displays statistics for only the selected device.
7. Scan the CPU chart for the distressed device, and look for the point where the cycles jumped up.

   Tip: *If you find a spike, you will want to focus in to narrow the time focus. There are two ways you can zoom in on an area of interest:*

   - Click either end of the focus element on the time selector to define the interval you want to examine.
   - Click and drag over the interval. A small magnifying glass pops up over the area you highlight. When you click the magnifying glass, the time selector focus is set to the area you highlighted.

   Note: *When you zoom in to focus on the area of interest, the focus changes for all charts on the Device Health overview screen.*

8. Make a note of both the host name of the BIG-IP device, and the time that the CPU cycles climbed.
   You have found a device that is in distress and identified the time that the issue started.
9. On the left, click **DASHBOARDS** > **Device** > **Traffic**.
   The Device Traffic overview screen opens.
10. On the Device Traffic overview screen, adjust the dimensions pane so that it fills up at least half of the screen.
11. In the dimensions pane, click the down arrow on the BIG-IP Host Names dimension to expand the list of BIG-IP devices.
12. In the Name column, click the magnifying glass icon (🔍), type the host name of the BIG-IP device noted in step 8, then click the magnifying glass icon again.
    The chart pane displays statistics for only the selected device.

13. Use the time selector controls to focus in on the time noted in step 8, and look through the traffic charts to see if there was a spike in traffic that corresponds to the spike in CPU cycles.
    If you find that spike, you have found the reason for the spike in CPU cycles. Traffic on that device is very high. You probably want to find out more about that traffic.
14. On the left, click **DASHBOARDS** > **Local Traffic** > **Virtual Servers**.
    The Virtual Servers overview screen opens.
15. On the Local Traffic Virtual Servers overview screen, adjust the dimensions pane so that it fills up at least half of the screen.
16. In the Name column, click the magnifying glass icon (🔍, type the host name of the BIG-IP device noted in step 8, then click the magnifying glass icon again.
    The chart pane displays statistics for only the selected device. Additionally, only the virtual servers that reside on that device are available on the Virtual Servers dimension.
17. In the dimensions pane, click the down arrow on the Virtual Servers dimension to expand the list.
18. In the Bytes Avg/s column, click one of the column headings (for example **C-->**) to sort the list of virtual servers by average traffic level in bytes per second on this virtual server.
19. Find the virtual server that has the highest number of new connections, and select it.
    The chart pane now displays statistics for the virtual server on the distressed device.

With the ID of the virtual server, you can figure out which application is triggering the traffic spike and figure out what your next step is from there.

Analyze application performance issues

Before you can analyze application performance data:

- There must be a BIG-IQ Data Collection Device configured for the BIG-IQ® device that manages your BIG-IP® devices.
- It is also a good idea, though not a requirement, to define the retention policy for the statistics data you are collecting.
- You will need to know the name of the virtual server that hosts the application that is having performance issues.

When you learn that an application is having performance issues, you can analyze the objects that serve that application to find the likely cause.

1. At the top of the screen, click **Configuration**.
2. On the left, expand **LOCAL TRAFFIC**.
3. Click **Virtual Servers**.
   The Virtual Servers screen opens showing a list of virtual servers managed by this BIG-IQ.
4. On the Virtual Servers screen, in the Filter in the upper right corner, type the name of the virtual server that is hosting the troubled application.
5. When you find the virtual server, select the virtual server name.
   The properties screen for the selected virtual server opens.
6. Click **View Statistics**.
   The Virtual Servers overview screen opens, but the only items selected are the virtual server you selected, and the BIG-IP device on which it runs.
7. Scan the statistics charts plotting data for the distressed server, and look for data (packet throughput) that indicates a problem.

   Tip: *There are two ways you can zoom in on an area of interest:*

- Click either end of the focus element on the time selector to define the interval you want to examine.
- Click and drag over the interval. A small magnifying glass pops up over the area you highlight. When you click the magnifying glass, the time selector focus is set to the area you highlighted.

If scanning the charts does not reveal an obvious cause, your next step might be to look for a troubled pool member or node.

8. On the Virtual Servers overview screen, click the back arrow (←) to return to the properties screen for the virtual server. Click it again to return to the Virtual Servers screen.
9. Find the virtual server name again, and select the check box that corresponds to it.
   At the bottom of the Virtual Server screen, a two panel preview pane opens displaying information about the virtual server.
10. On the right panel of the preview pane, under Related Items, click **Show**.
11. Select one of the Pool Members to display its properties screen, and then click **View Statistics**.
    The Pools & Pool Members overview screen opens, and again, the chart data that is displayed is only for the BIG-IP, pool, and pool name that you selected.

Analyze load balancing issues

Before you can analyze load balancing data:

- There must be a BIG-IQ data collection device configured for the BIG-IQ® device that manages your BIG-IP® devices.
- It is also a good idea, though not a requirement, to define the retention policy for the statistics data you are collecting.

When you get a report that an application is having performance issues, you can quickly determine if the cause is related to a load balancing problem.

1. At the top of the screen, click **Configuration**.
2. On the left, expand **LOCAL TRAFFIC**.
3. Click **Virtual Servers**.
   The Virtual Servers screen opens showing a list of virtual servers managed by this BIG-IQ.
4. On the Virtual Servers screen, in the filter in the upper right corner, type the name of the virtual server that is hosting the troubled application.
5. Find the virtual server name, and select the check box that corresponds to it.
   At the bottom of the Virtual Server screen, a two panel preview pane opens displaying information about the virtual server.
6. On the right panel of the preview pane, under Related Items, click **Show**.
7. Select one of the virtual servers pools to display its properties screen, and then click **View Statistics**.
   The Pools & Pool Members overview screen opens, and the chart data that displays is only for the pool you selected.
8. In the dimensions pane, click the down arrow on the **Pool Members** dimension to expand the list.
9. Click the name of each pool member until all of the members are selected.
10. Right click selected names, and select **Add Comparison Chart**.
    A new chart is added to the top of the chart pane. The chart plots the performance of the pool members, graphing the load balancing performance over time.
11. To change the comparison metric that plots for the selected pool members, click the down arrow in the title of the chart and select the new metric.

    You might want to try looking at the average bytes going to or from the server, or maybe the average new server connections.

12. If the virtual server has multiple pools, you might have to repeat the last four steps a couple of times to get the full picture.

Troubleshoot DNS traffic issues

Before you can troubleshoot DNS traffic performance issues:

- There must be a BIG-IQ data collection device configured for the BIG-IQ® that manages your BIG-IP® devices.
- It is also a good idea, though not a requirement, to define the retention policy for the statistics data that you are collecting.

When you learn that one of your DNS sync groups is having performance issues, you can analyze the DNS traffic to find the likely source of the issue.

1. At the top of the screen, click **Monitoring**.
2. On the left, click **DASHBOARDS** > **DNS** > **Overview**.
   The DNS overview screen opens to display dashlets and summary information about your DNS traffic.
3. Review the dashlets and summary charts for anomalous performance. When you spot a problem, you can find details using the other **DNS** options: **Traffic**, **GSLB**, **Services**, and **Attacks and Violations**. Explore the charts until you spot the most likely source of the performance issue.

Managing Audit Logs

About audit logs

You use audit logs to review changes in the BIG-IQ® system. All BIG-IQ system roles have read-only access to the audit log, and can view and filter entries. Any user with the appropriate privileges can initiate an action.

All API traffic on the BIG-IQ system, and every REST service command for all licensed modules, is logged in a separate, central audit log (`restjavad-audit.n.log`) which is located in `/var/log` on the BIG-IQ system.

Considerations when using the audit log

When using the audit log, consider the following:

- The audit log does not record an entry for every generation of a task. It only records an entry when the task status changes.
- When an object is deleted and then recreated with the same name, partition, and other information, the difference between those objects may show the deleted object as being the previous generation of the new object.
- By default, not all columns are displayed by the audit log to conserve space. To review what columns are displayed, click the gear icon in the upper right of the Audit Logging screen.

Actions and objects that generate audit log entries

BIG-IQ® records in the audit log all user-initiated changes that occur on the BIG-IQ system. A change is defined as when certain objects are modified, when certain tasks change state, or when certain user actions are performed. For example, when the admin account is used to log in to the BIG-IQ system, the audit log records the time, the user (admin), the action (New) and the object type (Login). The log does not include changes that occurred on BIG-IP® devices that were imported.

Changes to working-configuration objects generate audit log entries. In addition, these actions generate log entries:

- Creating or deleting a user account.
- Users logging in and logging out, including when the user is logged out due to inactivity.
- Creating or cancelling a device discovery or a device reimport.
- Creating a Network Security Change Verifications action to verify the changes to a specific BIG-IP device or group.
- Deleting a previously discovered device.
- Creating or deleting a deployment task.
- Creating a difference task.
- Creating, restoring, or deleting a snapshot.
- Editing some system information (such as editing a host name, a root password, a DNS entry, or an SNMP entry).

Audit log entry properties

The audit log displays the following properties for each log entry.

Property	Description
Source	IP address of the client machine that made the change. This property is blank for actions that were initiated by an internal process. For example, when a user invokes a deployment action, the deployment action then invokes a difference task to find the differences between the current configuration and the one to be deployed. The difference task has no Source IP address.
Service	Indicates whether the change was made by the internal object synchronization service. This service synchronizes shared objects, such as virtual servers, from the Local Traffic & Network service to the Network Security or Web Application Security services. • If a check mark is displayed, the change was made by the internal object synchronization service, and no IP address is shown in the Source column. The check mark is only displayed in the Network Firewall Audit Log or the Web Application Security Audit Log screens. • If a check mark is not displayed, the change was not made by the internal object synchronization service.
Time	Time that the event occurred. The time is the BIG-IQ system local time and is expressed in the format: mmm dd, yyyy hh:mm:ss (time zone); for example: `Apr 19, 2016 13:09:03(EDT).`
Node	Fully qualified domain name for the BIG-IQ system that recorded the event. This appears as the **Hostname** at the top of the BIG-IQ user interface.
User	Name of the account that initiated the action, such as an account named `Admin` for an administrative account.
Action	Type of modification. For operation changes, the action types include New, Delete, and Modify. For task changes, the action types include Start, Finish, Failed, and Cancelled.
Object Name	Object identified by a user-friendly name; for example: `newRule1`, `deploy-test`, or `Common/global`. When the name `RootNode` is listed, that indicates that the object is associated with a BIG-IP device. `RootNode` is typically seen when creating, deleting or updating log profiles, service policies, or firewall policies.
Changes	Indicates whether there was a change in the object. If **View** occurs in this column, there is a change to the object. To view the detailed differences of the change, click **View**.
Object Type	Classification for this action. When the type `Root Node` is listed, that indicates that the object is associated with a BIG-IP device. `Root Node` is typically seen when creating, deleting or updating log profiles, service policies, or firewall policies.
Parent	The administrative partition and name of the parent object. This property is displayed for firewall rules, logging profiles, and DoS profiles. For firewall rules, the parent shows the rule list, firewall, or policy that contains the rule. A change in a firewall rule often also affects the rule's parent object.
Parent Type	Class or group of the parent object.

Property	Description
Version	Version of the configuration object. Typically, when a configuration object changes, the version is increased by 1. However, other audit entries, such as those for finishing snapshot creation or finishing deployment, may increase the version by more than 1.

Viewing audit entry differences

In the audit log, when potential changes to an object are logged, the **View** link is shown in the Changes column for that entry. You can click **View** to examine the differences between generations of that object.

1. At the top of the screen, click **Monitoring**.
2. On the left, expand **LOGS**, then expand **Audit Logs**, and then , click the component that you want to view audit entries for.
3. To display differences for an object, click **View** in the Changes column.

   A popup screen opens, showing two columns that compare the differences between the two generations of the object in JSON. In these columns, additions to an object generation are highlighted in green, and differences are highlighted in gold.

   If the system cannot retrieve a generation of an object, the column displays either `Generation Not Available` or `Generation No previous generation`. Object information may not be available if it has been automatically purged from the system to conserve disk space, or if it has been deleted.

   The JSON difference displayed for a delete entry in the audit log shows the JSON difference from the previous operation because the generation identifier is not incremented when an object is deleted.
4. When you are finished, click **Close** on the popup screen to return to the Audit Logging screen.

Filtering entries in the audit log

You can use the Filter field at the top right of the Audit Logging screen to rapidly narrow the scope displayed, and to more easily locate an entry in the audit log.

- Filtering is text-based.
- Filtering is not case-sensitive.
- You can use wild cards, or partial text.
- All BIG-IQ® Centralized Management roles can filter entries.
- To clear the filter, click the **X** to the right of the search string in the **Filtered by** field on the left.

1. At the top of the screen, click **Monitoring**.
2. On the left, expand **LOGS**, then expand **Audit Logs**, and then , click the component that you want to view audit entries for.
3. Use the Filter field in the upper right corner to narrow your search:
   a) Select the field that you want to specify filter options for.
   b) Type the information specific to the object you want to filter on.
   c) Select **Exact** if you want to view only logs that completely match the filtering content you typed. Or, if you want to view any logs that include the filtering content, select **Contains**.
   d) Press **Enter**.

Option	Description
All	Specifies that all objects should be filtered using the filter text. When this option is used, both the user-visible and the underlying data are searched for a match, so you may see matches to your filter text which do not appear to match it.
Client Address	For **Filter**, type the IP address of the device that generates the logs. Log entries from devices with a different IP address will not be displayed.
Time	Type both a date and a time. Displayed times are given in the local time of the BIG-IQ system. Supported time formats are highly Web browser-dependent. Time formats other than those listed might appear to filter successfully but are not supported. Entering a single date and time results in a filter displaying all entries from the specified date and time to the current date and time. For time formats that use letters and numbers, enter the date time in one of the following formats: • mmm dd yyyy hh:mm:ss. Example: `Jan 7 2014 8:30:00` • mmm dd, yyyy hh:mm:ss (time zone). Example: `Apr 28, 2016 13:09:03(EDT)` • mmm dd, yyyy. Example: `Apr 28, 2016` • mmm dd, yyyy hh:mm:ss. Example: `Apr 28, 2016 16:09:06` • ddd mmm dd yyyy hh:mm:ss. Example: `Thu Jan 16 2014 11:13:50` For time formats that use only numbers, enter the date time in one of the following formats: • mm/dd/yy hh:mm:ss. Example: `01/01/16 12:14:15` • m/d/yy hh:mm:ss. Example: `1/1/14 12:14:15` • mm/dd/yyyy hh:mm:ss. Example: `1/1/2014 12:14:15`
Node	Type the node name in the filter.
User	Type the user account name in the filter.
Action: Operation	Type the operation action name in the filter. Operation actions include: New, Delete, and Modify. ***Note:*** *Search results for a search on values in the Action column may match additional hidden values since the underlying metadata is being searched.*
Action: Task Status	Type the task status action name in the filter. Task status actions include: Start, Finish, Cancelled, and Failed. ***Note:*** *Search results for a search on values in the Action column may match additional hidden values since the underlying metadata is being searched.*
Object Name	Type the full or partial name of the object in the filter. If a partition name is displayed, do not include it in the filter. For example, Common/AddressList_4 would be entered as `AddressList_4`. Because the device-specific object name includes the BIG-IP® host name, you can enter a full or partial device name to get all objects for a specific BIG-IP device.
Object Type	Type the object type in the filter.
Parent	Type the parent name in the filter. Only appears for rules to show the rule list, firewall, or policy that contains the rule.

Option	Description
Parent Type	Type the Parent Type name in the filter. Only appears when the Parent field contains a value.
Contains	Specifies that the filter text is contained within the object specified. When you select **Contains**: • If the filter text is a string, the filter text matches an entire string or only a part of a string. • If the filter text is an IP address, the filter text matches an IPV4 or IPV6 address that is the same as the filter text, or matches an IPV4 address range or subnet that includes the filter text. IPV6 addresses can not be found within a range or subnet. • If the filter text is a port number, the filter text matches a port number that is the same as the filter text, or matches a port number range that includes the filter text.
Exact	Specifies that the filter text is exactly contained within the object specified. When **Exact** is selected: • If the filter text is a string, the filter text matches only the entire string. • If the filter text is an IP address, the filter text matches only an IPV4 or IPV6 address that is the same as the filter text. • If the filter text is a port number, the filter text matches only a port number that is the same as the filter text.

The result of a search filter operation is a set of entries that match the filter criteria, sorted by time.

Customizing the audit log display

You can customize the audit log display to assist you in locating information faster.

- To customize the order of columns displayed, click any column header and drag the column to the location you want.
- To sort by column, click the name of the column you want to sort. Not all columns can be sorted. When sorting items in the Object Name column, partition names are ignored. For example, the object name `Common/rule1` would be sorted without the common partition name, as if it were named `rule1`.
- To resize columns, click the column side and drag it to the preferred location.
- To select what columns are displayed, click the gear icon in the upper right of the Audit Logging screen. In the popup screen, select columns you want to display and clear columns you do not want to display. Move your cursor away from the screen to dismiss it.

Managing audit log archive settings

You can view or change the audit archive settings. The archived audit log files are stored in the `/var/config/rest/auditArchive/` directory on the BIG-IQ® Centralized Management system.

Note:

Note: *Changing the audit archive settings while an archive is in progress could interrupt the current archive process. A subsequent archive operation will continue where the previous operation left off.*

1. At the top of the screen, click **Monitoring**.
2. On the left, expand **LOGS**, then expand **Audit Logs**, and then , click the component that you want to view audit entries for.
3. Click the **Archive Settings** button in the upper left of the Audit Logging screen to display the audit log settings.
4. Complete or review the properties and status settings, and click **Save**.

Property	Description
Retain Entries	Specifies the number of days to keep audit log entries. The field must contain an integer between 1 and 366. The default is 30.
Weekly Update	Specifies which days of the week to update the audit log. Select the check box to the left of each day that you want the audit log to be updated. The default is every day.
Start Time	Specifies when the audit archiving should begin. The default is 12:00 am.
Items Expired	Displays the read-only number of entries that have expired.
Last Error	If an error has occurred, displays the read-only error text for any errors found.
Last Error Time	If an error has occurred, displays a read-only value that contains the time the last error was found. The time in the field is the BIG-IQ Centralized Management system local time and is expressed in the format: ddd mmm dd yyyy hh:mm:ss, for example, `Fri Jan 17 2014 23:50:00`.

About archived audit logs

You can view or change how audit logs are archived by clicking the **Archive Settings** button on the Audit Logging screen.

Archived audit log files are stored in the `archive-audit.n.txt` file in the appropriate subdirectory of the `/var/config/rest/auditArchive` directory on the BIG-IQ® Centralized Management system:

- Network Security audit log: `/var/config/rest/auditArchive/networkSecurity/`
- Web Application Security audit log: `/var/config/rest/auditArchive/webAppSecurity/`
- Fraud Protection Service audit log: `/var/config/rest/auditArchive/websafe/`
- Local Traffic and Network audit log: `/var/config/rest/auditArchive/adc/`
- Device Management audit log: `/var/config/rest/auditArchive/device/`
- Access audit log:`/var/config/rest/auditArchive/access/`

Audit entries are appended to the `archive-audit.0.txt` file. When the `archive-audit.0.txt` file reaches approximately 800 MB, the contents are copied to `archive-audit.1.txt`, compressed into the `archive-audit.1.txt.gz` file, and a new empty `archive-audit.0.txt` file is created, which then has new audit entries appended to it.

Up to five compressed archived audit files can be created before those files begin to be overwritten to conserve space. The compressed audit log archive is named `archive-audit.n.txt.gz`, where n is a number from 1 to 5. As the audit log archives are created and updated, the content of the archives is rotated so that the newest archive is always `archive-audit.1.txt.gz` and the oldest is always the highest numbered archive, typically, `archive-audit.5.txt.gz`.

The file content rotation occurs whenever `archive-audit.0.txt` is full. At that time, the content of each `rchive-audit.n.txt.gz` file is copied into the file with the next higher number, and the content of `archive-audit.0.txt` is copied into `archive-audit.1.txt` and then compressed to create `archive-audit.1.txt.gz`. If all five `archive-audit.n.txt.gz`files exist, during the rotation the contents of `archive-audit.5.txt.gz` are overwritten, and are no longer available.

About audit logs in high-availability configurations

In high-availability (HA) configurations, there is a primary and secondary BIG-IQ® system. During failover, the audit log entries and the audit archive settings are copied from the primary to the secondary system before the secondary system becomes the new primary system.

However, archived audit logs are not copied from the primary to the secondary BIG-IQ system.

About the REST API audit log

The REST API audit log records all API traffic on the BIG-IQ® system. It logs every REST service command for all licensed modules in a central audit log (`restjavad-audit.n.log`) located on the system.

Note: *The current iteration of the log is named `restjavad-audit.0.log`. When the log reaches a certain user-configured size, a new log is created and the number is incremented. You can configure and edit settings in `/etc/restjavad.log.conf`.*

Any user who can access the BIG-IQ system console (shell) has access to this file.

Managing the REST API audit log

The REST API audit log contains an entry for every REST API command processed by the BIG-IQ® system, and is an essential source of information about the modules licensed under the BIG-IQ system. It can provide assistance in compliance, troubleshooting, and record-keeping. With it, you can review log contents periodically, and save contents locally for off-device processing and archiving.

1. Using SSH, log in to the BIG-IQ Network Security system with administrator credentials.
2. Navigate to the `restjavad` log location: `/var/log`.
3. Examine files with the naming convention: `restjavad-audit.n.log`.

   The letter *`n`* represents the log number.
4. Once you have located it, you can view or save the log locally through a method of your choice.

Access Reporting and Statistics

About Access and SWG reports

Access reports focus on session and logging data from Access devices (managed devices with APM licensed and provisioned). F5® Secure Web Gateway Services reports focus on user requests (for URLs or applications, for example) from Access devices with Secure Web Gateway Services provisioned. BIG-IQ® Centralized Management Access also supports high availability. Thus, users can view both Access and SWG reports on a secondary BIG-IQ system.

Access reports and SWG reports provide the following features.

- Reports on any combination of discovered devices, Access groups, and clusters
- Graphs for typical areas of concern and interest, such as cross-geographical comparisons or top 10 issues
- Tabular data to support the graphs
- Ability in some screens to drill down from summarized data to details
- Ability to save data to CSV files

Setup requirements for Access and SWG reports

Before you can produce Access reports and SWG reports, you must ensure that these tasks are already complete.

- Set up the BIG-IQ® Centralized Management data collection devices.
- Add the BIG-IP® devices to BIG-IQ inventory.
- Discover the devices. (Devices with the Access service configuration are what you need.)
- Run the data collection device configuration setup on the devices from the Access Reporting screen.

What data goes into Access reports for the All Devices option?

The **All Devices** option for Access reports includes data from the devices that are currently managed (discovered) in the BIG-IQ® system. This is in addition to data from devices that were managed at some point during the report timeframe, but that are not currently managed. With **All Devices** selected, if data from unmanaged devices exists, it displays in reports.

An unmanaged device might be unmanaged temporarily or permanently. Any time a configuration management change causes APM® to be undiscovered, the device and its data are moved to **All Devices** until APM is re-discovered on the device.

You cannot generate a report for an unmanaged device. However, you can generate a report for the timeframe when the device was managed, and then search the report for the unmanaged device name. In the Summary report, All Active Sessions includes the number of sessions that were active on the device when it became unmanaged. Those sessions stay in the Summary and in the Active sessions reports until the next session status update, which occurs every 15 minutes.

About upgrades affecting reports

When you upgrade a BIG-IQ® Centralized Management system without taking a snapshot, it deletes all reporting data, including both Access and SWG reports. After upgrading, users cannot obtain these reports from the BIG-IP® devices. To prevent the lost of reports, users should take an Elasticsearch snapshot before upgrading, and restore the snapshot after upgrading. For more information on elasticsnapshots, refer to *F5 BIG-IQ Centralized Management: Upgrading Logging Nodes to Version* x.x.

About the application dashboard

The Application Summary dashboard is your starting point to view and download general reports for BIG-IQ Access.

View the Application Summary dashboard

The BIG-IQ® Centralized Management Application Summary dashboard displays information regarding the applications linked to the system.

1. Log in to the BIG-IQ system with your user name and password.
2. At the top of the screen, click **Monitoring**.
3. On the left, select **DASHBOARDS** > **Access** > **Application Summary**.

The Application Summary screen opens, showing detailed information and charts for specific applications.

About application visibility

You can monitor your applications by viewing the BIG-IQ® Centralized Management Access user dashboard for data on which applications are linked to the BIG-IQ Access component. The system displays the top applications used and the application usage time. Administrators can expand the GUI for a specific application and view the following information:

- The application access history
- The users who use the application the most
- The access history
- The world map, showing where the user is access the application

About user visibility

You can monitor your user base by viewing the BIG-IQ® Centralized Management Access user dashboard for data on specific users. The system displays which users created the most sessions, were denied the most sessions, and had the longest total session duration. The administrator can enter a specific user name to get the following details for the user:

- User login locations on a world map.
- Total sessions, denied sessions, and session duration.
- Denied sessions.
- Top authentication failures, including AD Auth and LDAP only.
- Device type users used to log into the system.
- Reason the system terminated the session.

- Login history showing the success and failures over time.
- Most accessed applications.
- Most accessed URLs.
- Login failure attempts over time, sorted by the reason.
- Client session duration over time.
- Endpoint software.
- Network access reconnect, errors, and usage rates.

Managing a specific user in Access reporting

You can use the BIG-IQ® Centralized Management Access reporting tools to view the user dashboard for data on a specific user.

1. Log in to the BIG-IQ system with your user name and password.
2. Click **Monitoring** > **DASHBOARDS** > **Access** > **User Summary**.
   The User Summary screen displays, showing detailed information for specific users.

Running Access reports

For Access to have report data for a device, the device must have been added to the BIG-IQ® Centralized Management system, discovered, and had the Access remote logging configuration run for it.

You can create Access reports for any device with the APM® service configuration on it that has been discovered on the BIG-IQ system, whether or not the device is a member of an Access group. To create a report, you can select any combination of Access groups, clusters, and devices.

1. At the top of the screen, click **Monitoring**.
2. On the left, select **DASHBOARDS** > **Access**.
   A Summary report (for all devices and a default timeframe) starts to generate and display.
3. From the left, select any report that you want to run.
4. At the top left of the screen, from the **ACCESS GROUP/DEVICES** list, either select one of the first two options (**All Devices** and **All Managed Devices**) or, select one or more of the other options (<***`Access group name`***>, <***`Cluster display name`***>, and <***`Device name`***>).
   - **All Devices** Includes Access devices that are currently managed, and Access devices that were managed at one time but are not managed now. (A managed device is one that has been discovered with the APM service configuration.)
   - **All Managed Devices** Includes all Access devices that are currently discovered.
   - <***`Access group name`***> - Select to include all devices in the Access group.
   - <***`Cluster display name`***> - Select to include the devices in the cluster.
   - <***`Device name`***> - Select to include the device. You can select any device from **Managed Devices**, <***`Access group name`***>, or <***`Cluster display name`***>.
5. From the **TIMEFRAME** list, specify a time frame:
   - Select a predefined time period - These range from **Last hour** to **Last 3 months**.
   - Set a custom time period - Select **Between**, **After**, or **Before**, and click the additional fields that display the set dates and times that support your selection.
6. To save report data in a comma-separated values file, click the **CSV Report** button.
   A CSV file downloads.

Getting the details that underlie an Access report

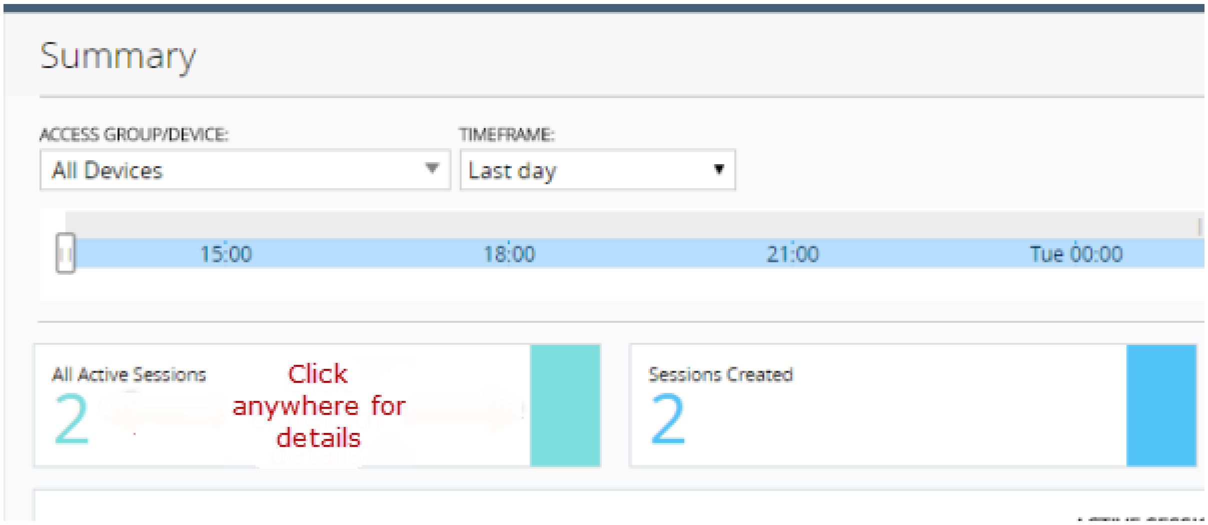
For Access to have report data for a device, the device must have been added to the BIG-IQ® Centralized Management system, discovered, and had the Access remote logging configuration run for it.

From the Summary report, and from most session reports, the initial display includes graphs that summarize the report data. You can get successively more detailed information by clicking a bar or a point on a graph or clicking a link if one is displayed on the screen.

1. Log in to the BIG-IQ system with your user name and password.
2. At the top of the screen, click **Monitoring**.
3. On the left, select **DASHBOARDS** > **Access**.

   The Summary report is an example of the type of report that presents high-level data, and provides access to underlying data.

   A Summary report (for all devices and a default timeframe) starts to generate and display.
4. Click anywhere in a summary to get more information.



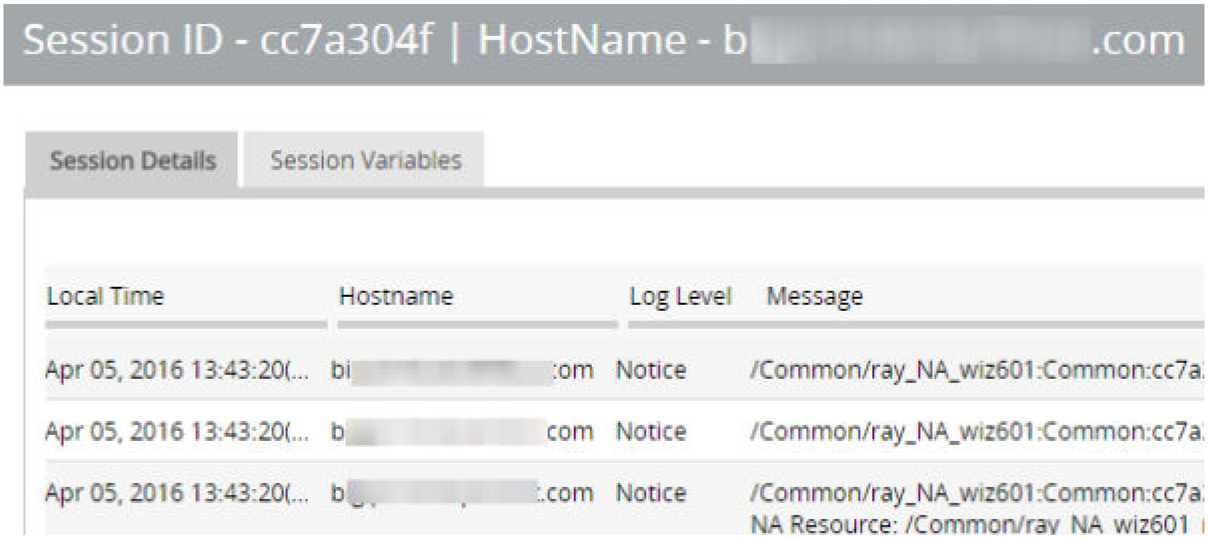
Summary

ACCESS GROUP/DEVICE: All Devices

TIMEFRAME: Last day

Figure 6: Top left portion of the Summary report display

   Additional graphs display, and supporting data displays in a table at the bottom of the screen.
5. If more details are available, click the bars in the graphs to display more details.
6. Scroll down to the table to view the supporting data.
7. If the table includes a **Session ID** field, click the link in that field to open the session details.



Session ID - cc7a304f | HostName - b[redacted].com

Local Time	Hostname	Log Level	Message
Apr 05, 2016 13:43:20(...	bi[redacted]:om	Notice	/Common/ray_NA_wiz601:Common:cc7a:
Apr 05, 2016 13:43:20(...	b[redacted]com	Notice	/Common/ray_NA_wiz601:Common:cc7a:
Apr 05, 2016 13:43:20(...	b[redacted].com	Notice	/Common/ray_NA_wiz601:Common:cc7a: NA Resource: /Common/ray_NA_wiz601

Figure 7: Session details popup screen (with addresses and host names blurred)

8. To change which records display on this screen, select a log level from the **LOG LEVEL** list at the top of the screen.

About the maximum number records for Access and SWG reports

When you run an Access report or an SWG report, Access can get up to 10,000 records to display to you. After you scroll to the end of those 10,000 records, Access displays a message. At that point, all you can do is select fewer devices or select a shorter timeframe.

Setting the timeframe for your Access or SWG report

For Access to have report data for a device, the device must have been added to the BIG-IQ® Centralized Management system, discovered, and had the Access remote logging configuration run for it.

Use the **TIMEFRAME** list at the top of any Access or SWG report to change the report time period.

1. Log in to BIG-IQ Centralized Management with your admin user name and password.
2. At the top of the screen, click **Monitoring**.
3. To set a predefined timeframe, select one of these from the **TIMEFRAME** list: **Last hour**, **Last day**, **Last week**, **Last 30 days**, **Last 3 months**.
4. To set a custom timeframe, select one of these from the**TIMEFRAME** list:
   - **Between**: Click each of the additional fields that display to select dates and times. The report displays the records between those dates and times.
   - **Before**: Click the additional fields that display to select a date and a time. The report displays the records before that date and time.
   - **After**: Click the additional fields that display to select a date and a time. The report displays the records after that date and time.

Access report problems: causes and resolutions

Problem	Resolution
A session is over, but it continues to display in the Active sessions report.	If a session starts when logging nodes are up and working, but terminates during a period when logging modes are unavailable, the session remains in the Active sessions report for 15 minutes. After 15 minutes, the session status is updated and the session is dropped from the report.
Active sessions are included in the Summary and Active sessions reports for a device that is no longer managed.	Sessions were active on a device when it was removed from an Access group and became unmanaged. Sessions that were active when the device became unmanaged remain counted in All Active Sessions on the Summary screen and stay in the Active sessions report until the next session status update, which occurs every 15 minutes.
A session is over, but **Session Termination** and **Session Duration** are blank in a session report.	If a session starts when logging nodes are up and working but terminates during a period when logging nodes are unavailable, the session termination is not recorded and the session duration cannot be calculated.

What can cause logging nodes to become unavailable?

Logging nodes are highly available, but it is still possible for them to become unavailable. This could occur, for example, if all logging nodes are on devices in the same rack in a lab, and the power to the lab shuts down.

Sessions

Running Session reports

For Access to have report data for a device, the device must have been added to the BIG-IQ® Centralized Management system, discovered, and had the Access remote logging configuration run for it.

You can create Session reports for any device with the APM® service configuration on it that has been discovered on the BIG-IQ system, whether or not the device is a member of an Access group. To create a report, you can select any combination of Access groups, clusters, and devices.

1. At the top of the screen, click **Monitoring**.
2. On the left, select **DASHBOARDS** > **Access** > **Sessions**.
   A Summary report (for all devices and a default timeframe) starts to generate and display.
3. From the left, select any report that you want to run.
4. At the top left of the screen, from the **ACCESS GROUP/DEVICES** list, either select one of the first two options (**All Devices** and **All Managed Devices**) or select one or more of the other options (<***`Access group name`***>, <***`Cluster display name`***>, and <***`Device name`***>).

- **All Devices** Includes Access devices that are currently managed, and Access devices that were managed at one time but are not managed now. (A managed device is one that has been discovered with the APM service configuration.)
- **All Managed Devices** Includes all Access devices that are currently discovered.
- <***`Access group name`***> - Select to include all devices in the Access group.
- <***`Cluster display name`***> - Select to include the devices in the cluster.
- <***`Device name`***> - Select to include the device. You can select any device from **Managed Devices**, <***`Access group name`***>, or <***`Cluster display name`***>.

5. From the **TIMEFRAME** list, specify a time frame:
   - Select a predefined time period - These range from **Last hour** to **Last 3 months**.
   - Set a custom time period - Select **Between**, **After**, or **Before**, and click the additional fields that display the set dates and times that support your selection.
6. To save report data in a comma-separated values file, click the **CSV Report** button.
   A CSV file downloads.

Stopping sessions on BIG-IP devices from Access

For Access to have report data for a device, the device must have been added to the BIG-IQ® Centralized Management system, discovered, and had the Access remote logging configuration run for it.

You can stop currently active sessions on BIG-IP® devices, using the Active sessions report on the BIG-IQ system.

1. Log in to the BIG-IQ system with your user name and password.
2. At the top of the screen, click **Monitoring**.
3. On the left, select **DASHBOARDS** > **Access**.
   A Summary report (for all devices and a default timeframe) starts to generate and display.
4. On the left, from **Sessions**, select **Active**.
   The screen displays a list of active sessions for all devices.
5. To display sessions for particular devices, groups, or clusters only, select them from the **ACCESS GROUP/DEVICE** list at upper left.
   The screen displays the active sessions for the selected devices.
6. To stop specific sessions only, select the sessions that you want to end and click **Kill Selected Sessions**.
7. To stop all sessions, click **Kill All Sessions**.

Running Secure Web Gateway reports

For Access to have report data for a device, the device must have been added to the BIG-IQ® Centralized Management system, discovered, and had the Access remote logging configuration run for it.Only a device with SWG provisioned on it can provide data for Secure Web Gateway reports.

You can create SWG reports for Access groups, clusters (in Access groups), or devices that you select from the Access groups and clusters (in Access groups) on the BIG-IQ system.

1. Log in to the BIG-IQ system with your user name and password.
2. At the top of the screen, click **Monitoring**.
3. On the left, select **DASHBOARDS** > **Access** > **Secure Web Gateway**.
   A Summary report (for all devices and a default timeframe) starts to generate and display.
4. From the left, select any report that you want to run.
5. From the **ACCESS GROUP/DEVICE** list at upper left, select **Managed Devices** or select one or more of these options:

- <***Access group name***> - Select to include all devices in the Access group.
- <***Cluster display name***> - Select to include the devices in the cluster.
- <***Device name***> - Select to include the device. You can select any device from **Managed Devices**, <***Access group name***>, or <***Cluster display name***>.

6. From the **TIMEFRAME** list, specify a time frame:
   - Select a predefined time period - These range from **Last hour** to **Last 3 months**.
   - Set a custom time period - Select **Between**, **After**, or **Before**, and click the additional fields that display the set dates and times that support your selection.
7. To save report data in a comma-separated values file, click the **CSV Report** button.
   A CSV file downloads.

About denied sessions

You can monitor the sessions that BIG-IQ® Centralized Management denies. By using the Access Monitoring option, you can view the following information:

- The history of denied sessions
- The reasons why sessions were denied
- The top denied users, sorted by session count
- The top authentication failures
- The top denied policies
- The top denied sessions by country of origin
- The top denied session by the virtual server
- The denied sessions, sorted by the client platform

Viewing denied sessions

You can use the BIG-IQ® Centralized Management Access reporting features to see which sessions were denied by the system, as well to create a report.

1. Log in to the BIG-IQ system with your user name and password.
2. Click **Monitoring** > **DASHBOARDS** > **Access** > **Sessions** > **Denied**.
3. From the **ACCESS GROUP/DEVICE** list at upper left, select **Managed Devices** or select one or more of these options:
   - <***Access group name***> - Select to include all devices in the Access group.
   - <***Cluster display name***> - Select to include the devices in the cluster.
   - <***Device name***> - Select to include the device. You can select any device from **Managed Devices**, <***Access group name***>, or <***Cluster display name***>.
4. From the **TIMEFRAME** list, specify a time frame:
   - Select a predefined time period - These range from **Last hour** to **Last 3 months**.
   - Set a custom time period - Select **Between**, **After**, or **Before**, and click the additional fields that display the set dates and times that support your selection.
5. To save report data in a comma-separated values file, click the **CSV Report** button.
   A CSV file downloads.

From here, you can view details regarding denied sessions and create a report.

Getting the details that underlie an SWG report

For Access to have report data for a device, the device must have been added to the BIG-IQ® Centralized Management system, discovered, and had the Access remote logging configuration run for it.Only a device with SWG provisioned on it can provide data for SWG reports.

From the Summary report, the initial display includes graphs that summarize the report data. You can get more detailed information by clicking a bar or a point on a graph to see additional graphs and tables with supporting entries.

1. Log in to BIG-IQ Centralized Management with your admin user name and password.
2. At the top of the screen, click **Monitoring**.
3. On the left, select **DASHBOARDS** > **Access** > **Secure Web Gateway**.
   The Summary starts to generate and display. A timeline and some summaries display across the top of the screen. Graphs display under the summaries. Each graph provide different views of the data.
4. Click any bar in a graph on the display to get more information.
   Additional graphs provide different views of the data, and supporting data displays in a table at the bottom of the screen.
5. If more details are available, click the bars in the graphs to display them.
6. Scroll down to the table to view the supporting data.

About VDI reports

You can monitor your virtual desktop infrastructure (VDI) by viewing the BIG-IQ® Centralized Management Access user dashboard for VDI applications, and creating a VDI report. The system displays the top VDI applications used and the application usage time. Administrators can expand the UI for a specific application, and view the following information:

- The top 10 VDI applications
- The top users for the VDI applications
- The application usage history

About network access reporting

You can use F5® BIG-IQ® Centralized Management to monitor the health of your network access connections. From the Network Access dashboard, you can view graphs and data for network access performance, reconnecting detail, errors, and usage rates. With the network access reporting feature, you gain full visibility of your network access usage information such as which users are request access, timestamps of the requests, and details of failures in their APM enviornments. All this allows you to troubleshooting your BIG-IP system deployments without logging into each BIG-IP device individually.

Note: *After you set up data collection devices, the BIG-IQ system requires approximately 10 minutes to process the event logs required to display network access reporting data. This applies to new setups as well as rolling and regular upgrades from BIG-IQ version 5.2/5.3 to 5.4.*

View the network access summary

View the Network Access Summary screen to see reporting details such as network sessions, connections, the number of bytes transferred.

1. At the top of the screen, click **Monitoring**.
2. On the left, select **DASHBOARDS** > **Access** > **Remote Access** > **Network Access** > **Network Access Summary**.
   The Network Access Dashboard screen opens.
3. Generate a report with a different scope by making a selection from the **ACCESS GROUP/DEVICE** list or the **TIMEFRAME** list, or both, then click **CSV Report**.

   You can use the summary screen to select a virtual server besides making a selection from either lists.

   A Report Download Status screen opens, downloading a CSV report to your local drive.

4. To view reporting details about the number of active users, click **Active Users**.
5. To view reporting details about the number of active connections, click **Active Connections**.
6. To view reporting details about the total number of reconnects, click **Total Reconnects**.
7. To view reporting details about the number of connectivity errors, click **Network Access Session Errors**.
8. Click the **Sessions** tab to display reporting details about network access sessions.
9. Click the **Connections** tab to display reporting details about network access connections.
10. Click the **Bytes Transferred** tab to display reporting details about the number of bytes transferred in network access connection.

About network access performance

The Network Access Performance screen gives you an overview of how your network access traffic is performing. BIG-IQ supports the following features:

- **Throughput over time** - Displays a graph showing the throughput to and from the client device in bits per second.
- **Active connections over time** - Displays a graph showing the average number of connections per hour.
- **New connections over time** - Displays a graph showing the average number of new connections per hour.

About network access reconnect

The Network Access Reconnect screen gives you an overview of your network access reconnects. BIG-IQ supports the following features:

- **Local Time** - Displays the local timestamp when the user reconnected to the network access connection.
- **Hostname** - Displays the BIG-IP system from which the network access connection originates.
- **Cluster** - Displays the BIG-IP APM cluster.
- **Session ID** - Click the session ID to open the Session Details screen, displaying session details and session variables.
- **User Name** - Displays the username of the reconnecting user.
- **Client IP** - Displays the IP address of the client device used for the reconnect.
- **Client OS** - Displays the operating system of the client device used for the reconnect.
- **Country** - Displays the country where the reconnect originates.
- **State** - Displays the geographical state where the reconnect originates.
- **Continent** - Displays the continent where the reconnect originates.
- **Client Application** - Displays the client application associated with the network access.

About network access errors

The Network Access Errors screen gives you an overview of your errors that occur during your active network access connections. BIG-IQ supports the following features:

- **Local Time** - Displays the local timestamp when error occurred.
- **Hostname** - Displays the BIG-IP system from which the network access error occurred.
- **Session ID** - Click the session ID to open the Session Details screen, displaying session details and session variables.
- **Error Message** - Displays the error message.
- **User Name** - Displays the username of the the user associated with the error.
- **Client IP** - Displays the IP address of the client device where the error occurred.

- **Client OS** - Displays the operating system of the client device where the error occurred.
- **Country** - Displays the country where the error occurred.
- **Virtual Server** - Displays the virtual server associated with the network access resource.

About network access usage

The Network Access Usage screen gives you an overview of your network access connection usage rates. BIG-IQ supports the following features:

View network access usage for the top 1000 users in the table:

- **User Name** - Displays the usernames of the top users by usage.
- **Total Connections** - Displays the total number of network access connections.
- **Total Bytes In** - Displays the total number of bytes received by the network access.
- **Total Bytes Out** - Displays the total number of bytes sent out by the network access.
- **Total Bytes Transferred** - Displays the total number of sent and received bytes.
- **Total Duration** - Displays the total duration when the network access connections for a user were active. When the user has multiple active connections at the same time, the total duration is the sum of the duration of those two connections.
- **Distinct Locations** - Displays the number of unique locations from where the network access usage originates.

View network access usage for the top 1000 locations in the table:

- **Country** - Displays the countries from where the network access usage originates.
- **State** - Displays the states in the countries from where the network access usage originates.
- **Total Connections** - Displays the total number of network access connections.
- **Total Bytes In** - Displays the total number of bytes received by the network access.
- **Total Bytes Out** -Displays the total number of bytes sent out by the network access.
- **Total Bytes Transferred** - Displays the total number of sent and received bytes.
- **Total Duration** - Displays the total duration when the network access connections for a user were active. When the user has multiple active connections at the same time, the total duration is the sum of the duration of those two connections.

About endpoint security check

You can use F5® BIG-IQ® Centralized Management to monitor the your endpoint security checks. From the Endpoint Software Summary dashboard, you can view graphs and tables showing how your system collects and verifies system information. With the endpoint software reporting feature, you gain full visibility of your software checks, products, and vendors. All this allows you to troubleshooting your BIG-IP system deployments without logging into each BIG-IP device individually.

About endpoint software summary

The Endpoint Software Summary screen gives you an overview of your endpoint checks. BIG-IQ supports the following features:

- **SOFTWARE CHECKS TYPES** - Displays the types of software checks.
- **TOP 10 USED PRODUCTS** - Displays the top ten products used.
- **TOP 10 USED VENDORS** - Displays the top ten vendors used.
- **Top 100 Products, Vendors Types by used count** - Displays the top 100 products and the type of vendors used.

About endpoint software details

The Endpoint Software Details screen a detailed table of your endpoint software checks. BIG-IQ supports the following features:

- **Local Time** - Displays the local timestamp when the endpoint check took place.
- **Hostname** - Displays the BIG-IP system from which the endpoint check originates.
- **Cluster** - Displays the BIG-IP APM cluster.
- **Session ID** - Click the session ID to open the Session Details screen, displaying session details and session variables.
- **Product Name** - Displays the name of the product with endpoint software.
- **Vendor Name** - Displays name of the vendor who supplies the product.
- **Version** - Displays the product version.
- **User Name** - Displays the logon name used to perform the endpoint check.
- **Client OS** - Displays the operating system where the endpoint check originates.
- **Continent** - Displays the continent where the endpoint check originates.
- **Country** - Displays the country where the endpoint check originates.
- **State** - Displays the state or province where the endpoint check originates.

Managing federation reports

Running OAuth reports

For Access to have report data for a device, the device must have been added to the BIG-IQ® Centralized Management system, discovered, and had the Access remote logging configuration run for it.Only a device with OAuth provisioned on it can provide data for OAuth reports.

You can create OAuth reports for Access groups, clusters (in Access groups), or devices that you select from the Access groups and clusters (in Access groups) on the BIG-IQ® Centralized Management system.

1. Log in to the BIG-IQ system with your user name and password.
2. At the top of the screen, click **Monitoring**.
3. On the left, select **DASHBOARDS** > **Access** > **Federation** > **OAuth**.
4. Select **Authorization Server**, **Client**, or **Resource**.
   A Summary report (for all devices and a default timeframe) starts to generate and display.
5. From the left, select any report that you want to run.
6. From the **ACCESS GROUP/DEVICE** list at upper left, select **Managed Devices** or select one or more of these options:
   - <***`Access group name`***> - Select to include all devices in the Access group.
   - <***`Cluster display name`***> - Select to include the devices in the cluster.
   - <***`Device name`***> - Select to include the device. You can select any device from **Managed Devices**, <***`Access group name`***>, or <***`Cluster display name`***>.
7. From the **TIMEFRAME** list, specify a time frame:
   - Select a predefined time period - These range from **Last hour** to **Last 3 months**.
   - Set a custom time period - Select **Between**, **After**, or **Before**, and click the additional fields that display the set dates and times that support your selection.
8. To save report data in a comma-separated values file, click the **CSV Report** button.

A CSV file downloads.

Monitoring the OAuth server performance

The Authentication Server Summary screen shows several charts that you can use to track the health of your authorization server role. Data appears when you configure statistics collection. Controls on this screen work together so you can fine-tune the statistics display.

1. Log in to the BIG-IQ system with your user name and password.
2. At the top of the screen, click **Monitoring**.
3. On the left, select **DASHBOARDS** > **Access** > **Federation** > **OAuth** > **Authorization Server** > **Server Performance**.
   The Authorization Server Peformance screen opens.
4. From the **ACCESS GROUP/DEVICE** list at upper left, select **All Managed Devices** or or one of the session-specific options.
5. From the **TIMEFRAME** list, specify a time frame:
   - Select a predefined time period - These range from **Last hour** to **Last 3 months**.
   - Set a custom time period - Select **Between**, **After**, or **Before**, and click the additional fields that display the set dates and times that support your selection.
6. From the **AUTHORIZATION SERVER** list, select an OAuth authorization server.
7. To save report data in a comma-separated values file, click the **CSV Report** button.
   A CSV file downloads.

Monitoring the OAuth token summary

The Token Summary screen shows several charts that you can use to track the health of your OAuth tokens. Data appears when you configure statistics collection. Controls on this screen work together so you can fine-tune the statistics display.

1. Log in to the BIG-IQ system with your user name and password.
2. At the top of the screen, click **Monitoring**.
3. On the left, select **DASHBOARDS** > **Access** > **Federation** > **OAuth** > **Authorization Server** > **Tokens**.
   The Authorization Server Peformance screen opens.
4. From the **ACCESS GROUP/DEVICE** list at upper left, select **All Managed Devices** or or one of the session-specific options.
5. From the **TIMEFRAME** list, specify a time frame:
   - Select a predefined time period - These range from **Last hour** to **Last 3 months**.
   - Set a custom time period - Select **Between**, **After**, or **Before**, and click the additional fields that display the set dates and times that support your selection.
6. From the **AUTHORIZATION SERVER** list, select an OAuth authorization server.
7. From the **GRANT TYPE** list, select an OAuth2 grant type.
8. To save report data in a comma-separated values file, click the **CSV Report** button.
   A CSV file downloads.

Running SAML reports

For Access to have report data for a device, the device must have been added to the BIG-IQ® Centralized Management system, discovered, and had the Access remote logging configuration run for it.Only a device with SAML provisioned on it can provide data for SAML reports.

You can create SAML reports for Access groups, clusters (in Access groups), or devices that you select from the Access groups and clusters (in Access groups) on the BIG-IQ® Centralized Management system.

1. Log in to the BIG-IQ system with your user name and password.
2. At the top of the screen, click **Monitoring**.
3. On the left, select **DASHBOARDS** > **Access** > **Federation** > **SAML**.
4. Select **SP Summary** or **IdP Summary**.
   A Summary report (for all devices and a default timeframe) opens, displaying chart data for assertions over time, the top SPs or IdPs with successful assertions, the top client IP addresses, the top subject values with successful assertions, and the top SP or IdPs with failed assertions.
5. From the **ACCESS GROUP/DEVICE** list at upper left, select **All Managed Devices** or or one of the session-specific options.
6. From the **TIMEFRAME** list, specify a time frame:
   - Select a predefined time period - These range from **Last hour** to **Last 3 months**.
   - Set a custom time period - Select **Between**, **After**, or **Before**, and click the additional fields that display the set dates and times that support your selection.
7. From the **SP** list, select a service provider.
8. To save report data in a comma-separated values file, click the **CSV Report** button.
   A CSV file downloads.
9. To view the successful SP assertions, click **Assertions Success**.
   The Successful Assertions screen opens, displaying data and statistics for the top 10 client IP's, platform distribution, geolocation distribution, subject values and SPs with successful assertions.
10. To view the failed SP assertions, click **Assertions Failed**.
    The Failed Assertions screen opens, displaying data and statistics for the top 10 client IP's, platform distribution, geolocation distribution, subject values and SPs with failed assertions.

Running SP assertion reports

For Access to have report data for a device, the device must have been added to the BIG-IQ® Centralized Management system, discovered, and had the Access remote logging configuration run for it.Only a device with SAML provisioned on it can provide data for SAML reports.

The SP Assertions screen shows several charts that you can use to track the health of your SAML SP assertions. Data appears when you configure statistics collection. Controls on this screen work together so you can fine-tune the statistics display.

1. Log in to the BIG-IQ system with your user name and password.
2. At the top of the screen, click **Monitoring**.
3. On the left, select **DASHBOARDS** > **Access** > **Federation** > **SAML**.
4. Select **SP Summary** > **SP Assertions Report**.
   The SP Assertions screen opens, displaying a table with assertion information.
5. From the **ACCESS GROUP/DEVICE** list at upper left, select **All Managed Devices** or or one of the session-specific options.
6. From the **TIMEFRAME** list, specify a time frame:
   - Select a predefined time period - These range from **Last hour** to **Last 3 months**.
   - Set a custom time period - Select **Between**, **After**, or **Before**, and click the additional fields that display the set dates and times that support your selection.
7. From the **SP** list, select a service provider.
8. To save report data in a comma-separated values file, click the **CSV Report** button.
   A CSV file downloads.

Running SP error reports

For Access to have report data for a device, the device must have been added to the BIG-IQ® Centralized Management system, discovered, and had the Access remote logging configuration run for it.Only a device with SAML provisioned on it can provide data for SAML reports.

The SP Errors screen shows several charts that you can use to track the health of your SAML SP errors. Data appears when you configure statistics collection. Controls on this screen work together so you can fine-tune the statistics display.

1. Log in to the BIG-IQ system with your user name and password.
2. At the top of the screen, click **Monitoring**.
3. On the left, select **DASHBOARDS** > **Access** > **Federation** > **SAML**.
4. Select **SP Summary** > **SP Error Report**.
   The SP Errors screen opens, displaying a table with error reports.
5. From the **ACCESS GROUP/DEVICE** list at upper left, select **All Managed Devices** or or one of the session-specific options.
6. From the **TIMEFRAME** list, specify a time frame:
   - Select a predefined time period - These range from **Last hour** to **Last 3 months**.
   - Set a custom time period - Select **Between**, **After**, or **Before**, and click the additional fields that display the set dates and times that support your selection.
7. From the **SP** list, select a service provider.
8. To save report data in a comma-separated values file, click the **CSV Report** button.
   A CSV file downloads.

Running IdP assertion reports

For Access to have report data for a device, the device must have been added to the BIG-IQ® Centralized Management system, discovered, and had the Access remote logging configuration run for it.Only a device with SAML provisioned on it can provide data for SAML reports.

The IdP Assertions screen shows several charts that you can use to track the health of your SAML IdPs assertions. Data appears when you configure statistics collection. Controls on this screen work together so you can fine-tune the statistics display.

1. Log in to the BIG-IQ system with your user name and password.
2. At the top of the screen, click **Monitoring**.
3. On the left, select **DASHBOARDS** > **Access** > **Federation** > **SAML**.
4. Select **IdP Summary** > **IdP Assertions Report**.
   The IdP Assertions screen opens, displaying a table with assertion information.
5. From the **ACCESS GROUP/DEVICE** list at upper left, select **All Managed Devices** or or one of the session-specific options.
6. From the **TIMEFRAME** list, specify a time frame:
   - Select a predefined time period - These range from **Last hour** to **Last 3 months**.
   - Set a custom time period - Select **Between**, **After**, or **Before**, and click the additional fields that display the set dates and times that support your selection.
7. From the **IdP** list, select an identity provider.
8. To save report data in a comma-separated values file, click the **CSV Report** button.
   A CSV file downloads.

Running IdP error reports

For Access to have report data for a device, the device must have been added to the BIG-IQ® Centralized Management system, discovered, and had the Access remote logging configuration run for it.Only a device with SAML provisioned on it can provide data for SAML reports.

The IdP Errors screen shows several charts that you can use to track the health of your SAML IdP errors. Data appears when you configure statistics collection. Controls on this screen work together so you can fine-tune the statistics display.

1. Log in to the BIG-IQ system with your user name and password.
2. At the top of the screen, click **Monitoring**.
3. On the left, select **DASHBOARDS** > **Access** > **Federation** > **SAML**.
4. Select **IdP Summary** > **IdP Error Report**.
   The IdPs Errors screen opens, displaying a table with error reports.
5. From the **ACCESS GROUP/DEVICE** list at upper left, select **All Managed Devices** or or one of the session-specific options.
6. From the **TIMEFRAME** list, specify a time frame:
   - Select a predefined time period - These range from **Last hour** to **Last 3 months**.
   - Set a custom time period - Select **Between**, **After**, or **Before**, and click the additional fields that display the set dates and times that support your selection.
7. From the **IdP** list, select an identity provider.
8. To save report data in a comma-separated values file, click the **CSV Report** button.
   A CSV file downloads.

Troubleshooting Access reporting

Overview: About troubleshooting Access reports

Access in the F5® BIG-IQ® Centralized Management monitoring dashboard displays statistics for applications and users that are managed by the BIG-IP® system. In some cases, data is missing in the dashboard. Missing data can include log message reports and session reports. You can troubleshoot this issue by doing the following tasks:

- Make sure the Elastic Search Cluster health status is operational.
- Active the Access service.
- Enable remote logging.
- Make sure the BIG-IP device is communicating to the data collection device.
- Recover any missing user names in the Sessions report and the Log Message report.
- Resolve unassigned cluster shards.

Check data collection device health

You can use the BIG-IQ® Data Collection Device Settings screen to review the overall health and status of the data collection devices you've configured. You can use the data displayed on this screen both before and after an upgrade to verify that your data collection device (DCD) cluster configuration is as you expect it to be.

1. At the top of the screen, click **System**, and then, on the left, click **BIG-IQ DATA COLLECTION** and select **BIG-IQ Data Collection Cluster**.

- Under Summary, you can view information detailing how much data is stored, as well as how the data is stored.
- Under Configuration, you can access the screens that control DCD cluster performance.

2. Inspect the DCD cluster details listed in the Summary and Configuration areas.

Sub-screen	What details are provided here?
Status	Look here for information about the current state of the cluster.
Nodes	Look here for information about the current state of the cluster nodes.
Indexes	Look here for information about the current state of the cluster indexes.
Shards	Look here for information about the current state of the cluster shards.
Cluster Settings	Displays information for the DCD cluster configured for this device.
External Storage & Snapshots	Displays summary information about the external storage location used to keep the backup snapshots you create for the DCD cluster configured for this device.
Logging Data Collection	Displays summary information for the event and alert log indices that have been configured for this DCD.
Statistics Data Collection	Displays details about the statistics data stored on this DCD.

This information provides a fairly detailed overview that describes the DCD cluster you have created to store data. After you complete an upgrade, you can check the health to verify that the cluster restored successfully.

Enable remote logging

Before you can configure remote logging for Access, you must first:

- Discover BIG-IP devices that are provisioned with the APM service.
- Configure one or more BIG-IQ data collection device.

Devices that you configure for remote logging send Access reporting and SWG log report data to the BIG-IQ Data collection device for storage and management.

1. At the top of the screen, select **Monitoring**.
2. Click **DASHBOARDS** > **Access** > **Remote Logging Configuration**.
   The Remote Logging Configuration screen displays.
3. From the HostName list, select the BIG-IP device for which you want to enable remote logging.
   The **Configure** button, once greyed out, becomes available.
4. Click **Configure**.

BIG-IQ Access sets up remote logging for the selected BIG-IP device. If an error occurs during the configuration, the Status field displays a message.

Check data collection device communication with the BIG-IP system

After checking the data collection device (DCD) health, activating relevant DCD services, and enabling remote logging, your F5® BIG-IQ® Centralized Management monitoring dashboard is still missing data such as log message reports and session reports. If this happens, the DCD might have routing issues with the BIG-IP system.

1. In your UNIX shell, type `ping <Listener Address>`

   Make sure BIG-IQ can communicate to the listener address on the DCD.

2. If the ping returns successfully, make sure the BIG-IP system can communicate with the listener by typing `telnet <listener address> <listener port>`.
3. If the telnet also returns successfully, use a tcpdump to check if the BIG-IP system sent out logs. Type `tcpdump -nvvv -i any -c 10000 -A 'port<listener port>'`.
   The tcpdump displays some log messages sent to the listener on the DCD.
4. If the tcpdump does not display any data, restart tmm apmd on the BIG-IP devices by typing `bigstart restart tmm apmd`.
5. If log messages and session reports are displaying in the dashboard reports, but the user name column is missing in the log messages, the BIG-IP system stopped sending apmd log messags. To fix this issue, type `bigstart restart apmd`.

Resolve unassigned cluster shards

An elastic search data cluster displays a color (red, green, or yellow) indicating the current status. A working cluster displays either a green state, or a yellow state if there is only one data collection device (DCD). A red status can indicate that one or more cluster shards are not assigned to the cluster, and can result in missing data in a report or failure to incorporate new incoming logs. Follow these steps to troubleshoot this issue.

1. From the TMSH command line, type `restcurl http://localhost:9200/_cluster/health`.
   The command line displays information on the cluster health. If the status output displays "`red`" and the unassigned shards output displays a number greater than zero, the issue might be the unassigned shards. However, if you have only one DCD, there are always unassigned shards because of replica shards and the lone log node. In this case, the status displays "`yellow`" and no action is needed.
2. If the status output is red and there are unassigned shards, the from the TMSH command line, type `curl "http://localhost:9200/_cat/nodes?v&h=host,ip,node.role,disk,name"`.
   The command line displays node information.
3. From the command line output, find the nodes with type `d` in the `node.role` column to identify the data nodes.
4. From the `disk` column, find the data node with the largest available disk space and note the node name in the `name` column..
5. Allocate the unassigned shards to the data node with the largest available disk space by saving the following code in the script file es_fix_unassignedshards.sh in your local BIG-IQ folder.

```
HOST=localhost
PORT=9200
TO_NODE=$1

curl "http://$HOST:$PORT/_cat/shards" | grep UNAS | awk '{print $1,$2}' | while read
var_index var_shard; do
 curl -XPOST "http://$HOST:$PORT/_cluster/reroute" -d "
    {
      \"commands\" : [
        {
          \"allocate\" :
            {
              \"index\" : \"$var_index\",
              \"shard\" : \"$var_shard\",
              \"node\" : \"$TO_NODE\",
              \"allow_primary\" : true
            }
        }
      ]
    }";

   sleep 5;
done
```

6. **6.** Run the script by typing in the command line `./es_fix_unassigedshards.sh <<node name>>`.

The cluster status should display green.

BIG-IP Application Visibility: How to configure the BIG-IP system

Overview: About the BIG-IP configuration for BIG-IQ application visibility

The F5® BIG-IQ® Centralized Management Application Summary dashboard displays statistics for applications and users that are managed by the BIG-IP® system. This includes the most requested applications, and how often individual users access the applications. For example, as an administrator, you can see the application summary report for the SharePoint application managed by the BIG-IQ system. You can use the report to track usage statistics, such as the request count for SharePoint and the most frequent users by request count. You can also adjust the time slider to see statistics for a certain time period.

To display these statistics, you must configure the BIG-IP system to classify the application traffic, create log messages, and send them to the BIG-IQ system. You can choose from two types of configurations:

Basic

A Basic configuration is your starting point to configure the BIG-IP system for application visibility. In some cases, you only need this option to generate the application logs and send them to the BIG-IQ system.

Advanced

In an Advanced configuration, after you configure a basic configuration and validate the reports, you might need to configure more BIG-IP resources such as classification presets and profiles. This situation typically occurs if there is not a predefined classification profile in the application that you want to display statistics and reports in.

Before you begin configuring application visibility, refer to *Access Reporting and Statistics*, in the *F5® BIG-IQ® Centralized Management: Monitoring and Reports* guide.

Note: *Configure both BIG-IP® LTM® and BIG-IP® APM®. Portal Access is not supported.*

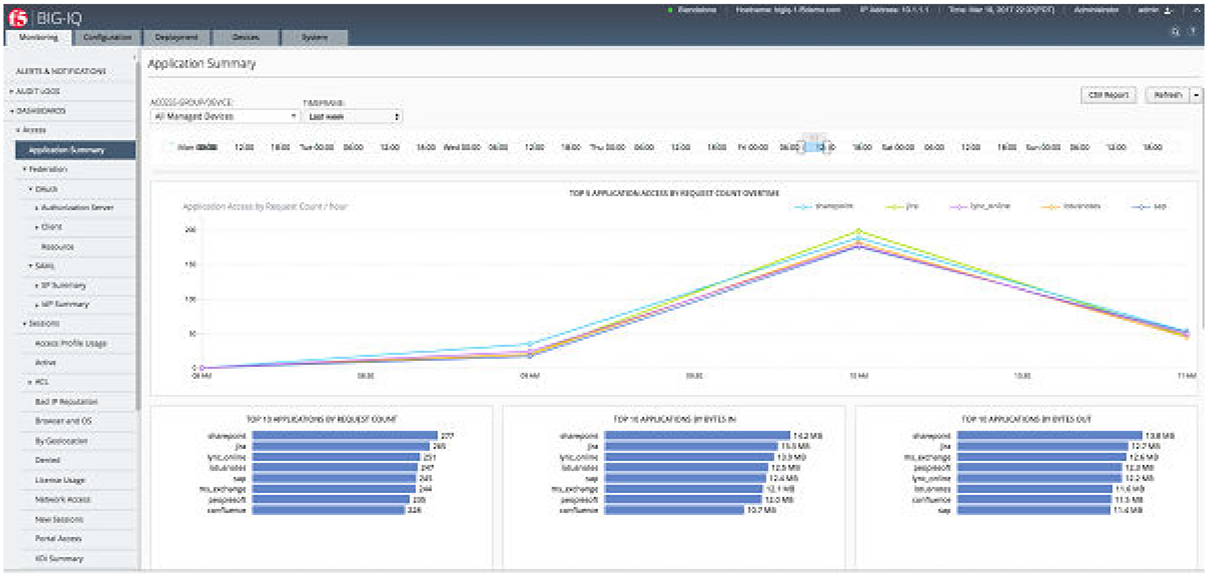


Figure 8: Sample Application Summary dashboard

Notice the length of time displayed by the line graph, dictated by the time slider above. Also notice the top ten applications, with SharePoint at number one. You can select an application and view the usage over time and the top users for that application.

View the Application Summary dashboard

The BIG-IQ® Centralized Management Application Summary dashboard displays information regarding the applications linked to the system.

1. Log in to the BIG-IQ system with your user name and password.
2. At the top of the screen, click **Monitoring**.
3. On the left, select **DASHBOARDS** > **Access** > **Application Summary**.

The Application Summary screen opens, showing detailed information and charts for specific applications.

What is a basic configuration?

The basic BIG-IP® system configuration for BIG-IQ® application visibility is when a classification profile is already available to the administrator. This situation occurs when you want to track predefined access applications in BIG-IQ, such as SharePoint, OWA, PeopleSoft, or Lotus Notes. When you configure the virtual server for one or more of these applications, the BIG-IP system has already configured a classification profile. For most other applications, this basic configuration does not apply, and you must create the classification profile as well as other necessary resources.

In some cases, you might want to define your own signatures. If so, even in a basic configuration, you must upload the signatures in Traffic Intelligence.

For a basic configuration, configure the following resources in both the BIG-IQ and BIG-IP systems:

- Enable remote logging in the Access area of BIG-IQ. Refer to the "BIG-IQ Centralized Management: Access" manual to learn how to configure remote logging.
- Update classification signatures in BIG-IP Traffic Intelligence.
- Configure a virtual server in BIG-IP Local Traffic.
- Attach an existing classification profile to the virtual server.

Note: *You must use BIG-IP version 13.0 as well as BIG-IQ version 5.2 or later.*

Note: *As part of the remote log configuration process, the system creates only the classification profile object name (classification _access). Because this classification profile is not attached to any virtual servers, you must add it to the virtual server used for applications that display reporting data. You should also enable the classification profile on the virtual server.*

About traffic signatures for application visibility

Classification signatures define different types of traffic that the BIG-IP® system can recognize through Traffic Intelligence. The system recognizes a predefined set of signatures for common applications and application categories that are updated periodically. You can download signature updates from F5 Networks, and schedule the system to automatically update the signatures (pull the updated signatures automatically). You can also manually install the classification signatures and updates, for example, if the BIG-IP system does not have Internet access.

Signatures are updated once a month and have the following requirements:

- Set up the DNS server on the BIG-IP system in order for the automatic updates to work.
- The management network should be on the Internet.

Scheduling automatic signature updates

You can set up the BIG-IP® system to automatically update the classification signatures. This ensures that the system always has the latest classification signature files.

1. On the Main tab, click **Traffic Intelligence** > **Applications** > **Signature Update**.
   The Signatures screen opens.
2. Click **Check for Updates** to manually upload a signature file update if one is available.
   You see the current date and time in the **Latest Update Check** setting of the Signature Definitions area.
3. To upload a signature file update, in the Signature Definitions area, click **Import Signatures**.
   The Applications screen displays a **Signatures File** field where you can select the new signature file.
4. To discard and remove any installed upgrades and reset the classification engine and signatures to factory default, click **Reset to Defaults**.
5. In the **Signatures File** field, click **Choose File** to navigate to the previously uploaded signatures file.
6. Click **Upload**.
   A message displays indicating whether your upload was successful.
7. For the **Automatic Updates Settings**, in the **Signature Update** screen, select **Enabled**.
8. From the **Update Schedule** setting, select **Daily**, **Weekly**, or **Monthly** to specify how often you want the system to check for updates.
9. Click **Update** to save your settings.

The signature updates take effect immediately.

Modify the virtual server for a basic configuration

Before you configure the virtual server in the BIG-IP® system, you must enable remote logging in the BIG-IQ® system.

For the BIG-IQ system to display statistics and reporting for an application such as SharePoint, OWA, or Lotus Notes, the application's virtual server must have a classification profile attached.

1. In the Main tab, click **Local Traffic** > **Virtual Servers** > **Virtual Server List**.
   A list of existing virtual servers displays.
2. Select the virtual server of the application that you wish to map to the BIG-IQ system.
   The virtual server editing (properties) screen opens.
3. From the **Configuration** list, select **Advanced**.
4. From the **Classification Profile** list, select `classification_access`.

   This classification profile was created by the BIG-IP system when you enabled remote logging in the BIG-IQ system.
5. Click **Update**.

You have added a classification profile to the virtual server.

What is an advanced configuration?

If you want to display statistics and reports using the Access feature of BIG-IQ® in an application that does not have a predefined classification profile, you must create the classification profile and attach it to the virtual server. This is considered an advanced configuration, and applies to most applications.

Because of this, you must configure the following resources in both BIG-IQ and BIG-IP® systems:

1. Enable remote logging in BIG-IQ Access. Refer to the *BIG-IQ Centralized Management: Access* manual to learn how to configure remote logging.
2. Create a classification policy in BIG-IP system Traffic Intelligence screens.

3. Create a new application from the Traffic Intelligence application list by customizing a category.
4. Update the existing classification preset or create a new preset.
5. Create a classification profile in the BIG-IP system's Local Traffic settings if you created a new classification preset. Otherwise, update the existing classification profile to include the existing preset.
6. Configure a virtual server in the BIG-IP system's Local Traffic settings.

Note: *Advanced configuration is introduced in BIG-IP version 13.1 and 13.0 Hotfix build 13.0.0 HF3.*

Note: *As part of the remote log configuration, only the classification profile object name (classification _access) is created. Because this classification profile is not attached to any virtual servers, you must add to the virtual server used for applications that display reports. You should also enable the classification profile on the virtual server.*

Creating a custom local traffic policy

You can create a custom local traffic policy to manage traffic assigned to a virtual server.

1. On the Main tab, click **Local Traffic** > **Policies**.

   For more information about local traffic policies, refer to *BIG-IP® Local Traffic Manager™: Implementations*.

   The Policy List screen opens.
2. Click **Create**.
   The New Policy List screen opens.
3. In the **Policy Name** field, type a unique name for the policy, for example `companyA`.
4. In the **Description** field, type descriptive text that identifies the policy definition.
5. From the **Strategy** list, select the action that the policy initiates when there are multiple rules that match.

Rule	Description
All	Uses the first or best strategy to resolve the conflict of rule match.
Best	Applies the actions of the rule specified in the list of defined strategies for the associated policy.
First	Applies the actions of only the first rule. This implies that the rule with the lowest ordinal, highest priority, or first in the list is applied.

6. From the **Type** list, select **CE Profile** to attach the policy to a CE profile.
7. Click **Create Policy**.
   This creates a policy that manages traffic assigned to a virtual server.

You have created a new local traffic policy for application visibility.

Creating a category

On the BIG-IP® system, you can create customized categories for classifying traffic if the predefined categories are not sufficient for your needs. For example, if you plan to create new application types unique to your organization, you can create a category to group them together. Alternatively, you can add an existing category to your application list.

1. On the Main tab, click **Traffic Intelligence** > **Applications** > **Application List**.
   The Applications screen displays a list of the supported classification categories.
2. On the Main tab, click **Traffic Intelligence** > **Categories** > **Category List**.
   The Category list screen opens.
3. Click **Create**.

The New URL Category screen opens.

4. In the **Name** field, type a name for the classification category.
5. In the **Description** field, type optional informative text.
6. In the **Category ID** field, type an identifier for this category, a unique number.
7. In the **Application List** setting, select applications from the list and use the Move buttons to move applications from one list to the other.
8. Click **Finished**.

You have created custom applications to handle traffic.

Create a classification application

The BIG-IP® system classifies many categories of traffic, and specific applications within those categories. You can create a new classification application, and determine which categories and applications of traffic the system can classify.

1. On the Main tab, click **Traffic Intelligence** > **Applications** > **Application List**.
   The Applications screen displays a list of the supported classification categories.
2. To view the applications in each category, click the **+** icon next to the category.
3. To view or edit the properties of the application or category, click the name to open its properties screen.

   Tip: *Here you can view the application or category ID number.*
4. Click **Create**.
5. In the **Name** field, type a name for the classification application.
6. In the **Description** field, type a descriptive text identifying the classification application.
7. In the **Application ID** field, type the identifier for a category, a new, unique number.
8. From the **Category** list, select an existing category or a category that you created.
9. Click **Finished**.

About presets and profiles

In BIG-IQ® application visibility, as part of the advanced configuration, there are two ways to configure the BIG-IP® classification preset and classification profile.

- You can use the existing classification preset, and make sure it is associated with the current classification profile.
- You can create a new classification preset, but you must also associate it with a new classification profile.

Updating classification presets

On the BIG-IP® system, you can update classification preset settings for a classification policy that you have previously created. Alternatively, you can create a new preset for application visibility.

1. On the Main tab, click **Traffic Intelligence** > **Presets**.
   The Presets screen displays a list of the supported classification categories.
2. From the preset list, select the preset **CE**.
3. From the **Policies** setting, move policies from the **Available** list to the **Enabled** list.
4. Click **Update**.

Updating a classification profile

If you update the existing classification preset, update the existing classification profile and attach the existing preset. In the profile, you can change which virtual servers and which categories of traffic are included in the classification statistics.

1. On the Main tab, click **Local Traffic** > **Profiles** > **Classification**.
   The Classification screen opens.
2. Click the **Create**.
   The New Classification Profile screen displays.
3. In the **Name** field, type a name for the classification profile.
4. In the **Description** field, click the check box and type a description for the profile.
5. From the **Parent Profile** dropdown list, select an existing profile from which this profile is derived.

   This profile inherits settings from the parent profile.
6. Click the check box next to **Custom**.
7. From the **Preset** dropdown list, select the preset **CE**.
8. From the **Log Publisher dropdown** list, select **access-gpa-log-publisher**.
9. Click **Finished**.

The BIG-IP system classifies traffic for the virtual servers and categories specified in the Classification profile.

Creating classification presets

On the BIG-IP® system, you can create classification preset settings for a classification policy that you have previously created.

1. On the Main tab, click **Traffic Intelligence** > **Presets**.
   The Presets screen displays a list of the supported classification categories.
2. Click **Create**.
   The New Presets screen opens.
3. In the **Name** field, type a name for the application.
4. In the **Description** field, type optional descriptive text for the classification presets.
5. For the **Policy** setting, move the classification policies from **Available** list to the **Selected** list, to create a new preset.
6. In the **Allow Reclassification** list, **Enabled** is the default selection.
7. In the **Flow Bundling** list, **Enabled** is the default selection.
8. In the **Cache Results** list, **Enabled** is the default selection.
9. Click **Finished**.

Creating a classification profile

If you create a new classification preset, you must create a new classification profile and attach the preset. In the profile, you can change which virtual servers and which categories of traffic are included in the classification statistics.

1. On the Main tab, click **Local Traffic** > **Profiles** > **Classification**.
   The Classification screen opens.
2. Click the **Create**.
   The New Classification Profile screen displays.
3. In the **Name** field, type a name for the classification profile.
4. In the **Description** field, click the check box and type a description for the profile.
5. From the **Parent Profile** dropdown list, select an existing profile from which this profile is derived.

   This profile inherits settings from the parent profile.
6. Click the check box next to **Custom**.
7. From the **Preset** dropdown list, select the new preset that you created previously.
8. From the **Log Publisher dropdown** list, select **access-gpa-log-publisher**.
9. Click **Finished**.

The BIG-IP system classifies traffic for the virtual servers and categories specified in the Classification profile.

Modify the virtual server for an advanced configuration

Before you configure the virtual server in the BIG-IP® system, enable remote logging in BIG-IQ® and create a classification profile.

For the Access feature of BIG-IQ to display statistics and reporting for an application such as SharePoint, OWA, or Lotus Notes, the application's virtual server must have a classification profile attached.

1. In the Main tab, click **Local Traffic** > **Virtual Servers** > **Virtual Server List**.
   A list of existing virtual servers displays.
2. Select the virtual server of the application that you want to map to the BIG-IQ system.
   The virtual server editing screen opens.
3. From the **Configuration** setting, select **Advanced**.
4. From the **Classification Profile** list, select the classification profile associated with the advanced configuration use case.
5. Click **Update**.

You have added a classification profile to the virtual server.

How much memory does application visibility need?

In the BIG-IP® system configuration for BIG-IQ® application tracking reporting, you do not need to allocate separate memory resources to enable the application visibility functionality. The runtime memory consumption depends on the amount of traffic processed, such as concurrent TCP flows.

Application visibility troubleshooting commands

Type these commands in the BIG-IP® UNIX shell to start and stop debugging and logging.

Command	Description
tmctl gpa_classification_stats	Displays classification results in a table that lists all applications that were classified, the number of flows, the bytes in, and the bytes out.
tmsh modify sys db tmm.cec.log.level value Debug **tmsh modify sys db tmm.gpa.log.level value Debug**	Generates debug logs. The log messages are stored in `/var/log/tmm`.
tmsh modify sys db tmm.cec.log.level reset-to-default **tmsh modify sys db tmm.gpa.log.level reset-to-default**	Stops debug log messages.

Managing Security Reports

About security reporting

Reporting for BIG-IQ® Network Security

You can use BIG-IQ® Network Security Reporting to view reports for managed BIG-IP® devices that are provisioned for Application Visibility and Reporting (AVR). Reports can be for a single BIG-IP device or can contain aggregated data for multiple BIG-IP devices (that are of the same BIG-IP device version).

Network Firewall, DoS and IP Intelligence reports can be created. Analytic reports provide detailed metrics about application performance such as transactions per second, server and client latency, request and response throughput, and sessions. Metrics are provided for applications, virtual servers, pool members, URLs, specific countries, and additional detailed statistics about application traffic running through one or more managed devices. You can view the analytics reports for a single device, view aggregated reports for a group of devices, and create custom lists to view analytics for only specified devices.

Reporting for BIG-IQ® Web Application Security

You can use BIG-IQ® Web Application Security Reporting to view reports for managed BIG-IP® devices that are provisioned for Application Visibility and Reporting (AVR). Similar to the availability of the AVR reporting on a single device, you have the ability to get visibility into application traffic passing through a single managed BIG-IP device or an aggregated system (aggregated data for multiple BIG-IP devices.

You can generate reports and charts in the following areas:

- Application. You can view information about requests based on applications (iApps), virtual servers, security policies, attack types, violations, URLs, client IP addresses, IP address intelligence (reputation), client countries, severities, response codes, request types, methods, protocols, viruses detected, usernames, and session identification numbers.
- Anomalies. You can view charts of statistical information in graphs about anomaly attacks, such as brute force attacks and web scraping attacks. You can use these charts to evaluate traffic to the web application, and to evaluate the vulnerabilities in the security policy.
- DoS. If you have configured DoS protection on the BIG-IP system, you can view charts and reports that show information about DoS attacks and mitigations in place on the system.

Monitoring Active Firewall Policies

View active firewall policies

You use the Active Policy screen to view summary information about the firewall policies and rules that are currently active on BIG-IP® devices.

1. Click **Monitoring** > **REPORTS** > **Security** > **Network Security** > **Active Firewall Policies**.
2. Review the firewall policies, including on what BIG-IP devices they are active.
3. To review the rules and rule lists in a policy, click the policy name.
   The screen displays rules and rule lists in the policy.
4. To edit a rule or rule list, click the name of the rule or rule list.

Active firewall policy rule properties

This table describes the rule properties shown for a firewall policy that is active on a BIG-IP device.

Column	Description
#	Specifies the evaluation order of the rule within the policy. Rules are evaluated from the lowest number to the highest. If a rule is contained within a rule list, it will be numbered after the decimal point. For example, a policy with 3 rules, followed by a rule list containing 2 rules, followed by another rule outside of the rule list, would be numbered as: `1, 2, 3, 4, 4.1, 4.2, 5`. In the example, 4 represents the rule list, and 4.1 and 4.2 are the evaluation order of the rules within that rule list.
Rule Name	Specifies the name of the rule. This contains a reference to the rule list when the row contains a rule list. You can click the rule name for more information.
Rule List Name	Specifies the name of the rule list that contains one or more rules. This is blank when the row contains a rule.
Action	Specifies the action taken when the rule is matched, such as whether it is accepted or rejected.
Protocol	Specifies the IP protocol used by the rule to compare against the packet.
Log	Specifies whether the firewall software should write a log entry for any packets that match this rule.
State	Specifies the activity state of the rule, such as whether it is enabled or disabled.

Monitoring Firewall Rules

About firewall rule monitoring

In BIG-IQ™ Network Security, you can monitor:

- Firewall rule statistics, such as the number of times inbound network traffic matches a firewall rule on a BIG-IP™device (also referred to as a firewall rule hit count) as well as the rule overlap status.
- Firewall rule compilation statistics for a set of rules associated with a firewall context on a BIG-IP device.

You access this firewall rule monitoring by selecting **Network Security** from the BIG-IQ menu and then clicking **Monitoring**.

You can generate reports about firewall rules by selecting **Network Security** from the BIG-IQ menu and then clicking **Policy Editor**, and then selecting **Firewall Rule Reports**.

Monitoring firewall rule statistics and hit counts

You can monitor firewall rule statistics and hit counts on one or more BIG-IP™ devices using Network Security monitoring.

***Note:** Firewall rule statistics are collected for the rules in the enforced policy associated with a firewall, but not the rules in a staged policy.*

***Note:** If a virtual server, route domain or self IP is created using the BIG-IQ™ system, firewall statistics cannot be collected until the changes are deployed to the device and reimported.*

1. Log in to the BIG-IQ system with your user name and password.
2. At the top left of the screen, select **Network Security** from the BIG-IQ menu.
3. Click **Monitoring**.
4. Click **Firewall Rule Statistics**.
   The Firewall Rule Statistics screen opens and displays a list of firewall contexts, including their name, partition, type, and on what BIG-IP device they occur.
5. Click the name of the firewall context to monitor.
6. The Firewall Rule Statistics page for that firewall context displays.

   The following information is listed in the named columns for each firewall rule on the BIG-IP device:

   - Rule Name specifies the name of the rule used in the policy. If not listed, the rule is not running.
   - Rule List Name specifies the name of the rule list if the rule is in a rule list.
   - Rule specifies the name of the rule within a rule list. If the rule is not in a rule list, this field is blank.
   - Overlap Status specifies whether the rule overlaps with another rule.
   - Hit Count specifies the number of times the rule has been matched.
   - Last Hit Time specifies when the rule was last matched.

Monitoring firewall rule compilation statistics

You can monitor rule compilation statistics on one or more BIG-IP™ devices using Network Security monitoring. This information is similar to what is displayed when using the `tmsh show security firewall container-stat` command.

***Note:** If a firewall context references a policy that is both staged and enforced, there will be two entries in the compilation statistics: one for the enforced policy and one for the staged policy.*

1. Log in to the BIG-IQ system with your user name and password.
2. At the top left of the screen, select **Network Security** from the BIG-IQ menu.
3. Click **Monitoring**.
4. Click **Firewall Compilation Statistics**.
   The Firewall Compilation Statistics screen opens and displays the list of BIG-IP devices managed by the BIG-IQ system, including their network name, IP address, and BIG-IP device version.
5. Click the name of the BIG-IP device to monitor.
6. The Firewall Compilation Statistics page for that BIG-IP device displays.

   Depending on the version of the BIG-IP device, the following information, or a subset of this information, may be listed in the named columns for the one or more firewall rules within the specified firewall context on the BIG-IP device:

   - **Context Name** specifies the context name associated with the one or more rules, such as `/Common/global-firewall-rules`.
   - **Context Type** specifies the firewall context type associated with the one or more rules, such as global or self IP.
   - **Policy Name** specifies the name of the policy associated with the one or more rules.
   - **Policy Type** specifies type of policy associated with the one or more rules, such as enforced or staged.
   - **Rule Count**Specifies the number of rules compiled for this BIG-IP device context, such as 30. This count includes rules in rule lists as well as rules that are not in rule lists.
   - **Compile Duration** specifies the amount of time required to compile the rules, expressed as `hours:minutes:seconds`.
   - **Overlap Check Duration** specifies the amount of time required to check overlapping rules, expressed as `hours:minutes:seconds`.
   - **Size** specifies the size of the compiled rules in bytes.
   - **Max Memory** specifies the maximum amount of memory consumed by the rules in bytes.
   - **Activation Time** specifies when the rules are activated and available for use.

Managing Firewall Rule Reports

About firewall rule reports

You can generate different types of firewall rule reports for selected BIG-IP® devices in either CSV or HTML format. These reports capture information similar to that gathered using the firewall rule monitoring. The types of reports you can generate include:

- Stale Rule Report. Creates a report on firewall rules that are not being used on the BIG-IP device.
- Overlap Status Stats Report. Creates a report on firewall rules that are overlapping on the BIG-IP device.
- Compilation Status Report. Creates a report on the compilation of firewall rules on the BIG-IP device.

Creating firewall rule reports

You create firewall rule reports to capture statistics about firewall rules in a report format.

1. Navigate to the Firewall Rule Reports screen: Click **Monitoring** > **REPORTS** > **Security** > **Network Security** > **Firewall Rule Reports**.
2. Click **Create**.
   The New Firewall Rule Report screen opens.
3. Type a name for the report in the **Name** field.
4. Type an optional description for the report in the **Description** field.
5. Select a report type from those listed in the **Report Type** field.

   You can generate these types of reports::

   - Stale Rule Report
   - Overlap Status Stats Report
   - Compilation Status Stats Report

   If the **Stale Rule Report** report type is selected, the screen displays the Stale Rule Criteria property, otherwise that property is not displayed.
6. If you select **Stale Rule Report**, you can refine the report using the options listed in the **Stale Rule Criteria** setting:

   - To specify that the report should include only rules with a hit count less than the number specified, select **Rules with count less than** and specify a number in the provided field.
   - To specify that the report should include only rules that have not been hit since the date specified, select **Rules that haven't been hit since** and specify a date in the provided field.
7. From the **Available Devices** setting, select the BIG-IP devices or device group to use for the report:

   - Select **Group** and select a group of BIG-IP devices from the list.
   - Select **Device** and select individual BIG-IP devices by moving them from the **Available** list to the **Selected** list.
8. Save the report:

   - Select **Save** to save the report. The system displays the Firewall Rule Reports page for that one report, and generates the report data.
   - Select **Save & Close** to save the report. The system displays the Firewall Rule Reports page that lists all reports, and generates the report data.

9. Select the format for the report:

   - Select **CSV Report** to have the report formatted as a CSV file.
   - Select **HTML Report** to have the report formatted as an HTML file. The HTML file is displayed in the Web browser when complete.

   You can save or print these reports.

Deleting firewall rule reports

You can delete firewall rule reports that are no longer needed.

1. Go to the Firewall Rule Reports screen: Click **Monitoring** > **REPORTS** > **Security** > **Network Security** > **Firewall Rule Reports**.
2. Select one or more reports to delete, and click **Delete**.
   The reports are deleted from the list on the Firewall Rule Reports screen.

Managing Firewall Packet Traces

About firewall packet traces

You can create and view packet traces to visually review your firewall settings. You can click the graphics in the trace report to see detailed results of the packet trace for each firewall component.

Create firewall packet traces

You create packet traces to trace and review your network security firewall settings.

1. Click **Monitoring** > **REPORTS** > **Security** > **Network Security** > **Packet Traces**.
2. Click **Create**.
   The Packet Parameters screen opens.
3. In the **Name** setting, type a name for the packet trace.
4. In the **Devices** setting, select one or more BIG-IP devices and source VLANs to use.

   Click **+** to add additional devices. Click **X** to remove the device in the row.
5. In the **Protocol** setting, select the protocol for the packet you want to trace. The other configuration settings change based on the protocol you select.
6. In the **TCP Flags** setting, select one or more flags to set in the packet trace. This setting is used only when the TCP protocol is selected.
7. In the **Source IP Address** setting, type the IP address to identify as the packet source.
8. In the **Source Port** setting, type the port to identify as the packet source. This does not apply to ICMP packets.
9. In the **TTL** setting, type the TTL (Time to Live) for the traced packet, in seconds.
10. In the **Destination IP Address** setting, type the IP address to which you want to send the packet for the packet trace.
11. In the **Destination Port** setting, type the port to which you want to send the packet for the packet trace. This does not apply to ICMP packets.
12. In the **Use Staged Policy** setting, select whether to use a staged policy, if one exists, for the packet.
13. In the **Trigger Log** setting, select whether to write a log message based on the packet from the packet trace.
14. Click **Run Trace**.
    The packet is traced and the results are displayed on the screen.
15. In the Trace Results area, review the trace diagram created by running the trace.
    - Review the colors of the graphics for each network security component.
      - Green graphics indicate rules that were evaluated and allowed the traffic to pass, including whitelist matches and Allow firewall, DoS, and IP intelligence matches.
      - Red graphics indicate packets that were evaluated and dropped, or that matched firewall or IP intelligence rules.
      - Gray graphics indicate packets that did not match a rule of the type indicated.
    - Click each graphic to see detailed results of the packet trace for that component.

Viewing Event Logs in Web Application Security

About event log viewing

You can view Web Application Security event logs to review applications and server activities. BIG-IQ® Centralized Management enables a single view of all filters and log entries (and details for each entry) from multiple BIG-IP® devices.

You use tags and filters to allow you to select which events to view.

- Filters allow you to select the events to view by constructing a query that the events must match.
- You can assign tags to events to label them, so that you can use that label in queries.

Before you can view events, event logging must be configured as follows.

1. Discover and activate a BIG-IQ Data Collection Device.
2. Configure a BIG-IP device to collect event logs and send them to the BIG-IQ Centralized Management Data Collection Device. Part of this configuration includes a virtual server configured with a logging profile.
3. Configure a logging profile for Web Application Security, assign it to a virtual server, and deploy it to the BIG-IP device that has been configured to collect log events. A *logging profile* is used to determine which events the system logs, and where, and the format of these events. It then directs security events to a BIG-IQ Data Collection Device, and the BIG-IQ Centralized Management system retrieves them from that node.

View event logs and define filters and tags

You can review Web Application Security events on applications and servers from one or more BIG-IP® devices. By default, the events are filtered to show only illegal requests. You can use the Web Application Security Event Logs screen to define tags and filters to help you find meaningful events.

1. Click **Monitoring** > **EVENTS** > **Web Application Security** > **Events**.
2. To create and apply tags to events, select the events using the check box to the left, and click **Tags** above the event list.

   A dialog box opens.

   - To create a tag, type the tag name in the provided field and click +.
   - To apply a tag to the selected events, select the check box to the left of the tag and click **Apply**.
3. To create filters, click the filter icon to the left of the Filter field in the upper right of the screen. In the dialog box that opens, click **Create**.

   The New Filter dialog box opens.

   a) In the **Filter Name** setting, enter a name.
   b) In the Query Parameters area, supply those parameter settings you want to be part of the filter. Note that as you enter parameter settings, they are used to construct the filter query in the Query Expression area.
   c) Save your work.
   The new filter is listed on the Filters screen.
4. To export selected events as a CSV file, select the event using the check box to the left, and click **Export**.
5. To display only events that contain a specified string, type that string in the Filter field in the upper right of the screen.

6. To see details of an event log entry, click in the event entry row.
   A screen on the right opens and shows details of the event.
7. In the details screen, you can specify the kind of information to see.
   - You can specify compact or full information. At the top of the screen, click **Compact** for summary information, or click **Full** for complete information.
   - You can specify either request or response information. Click **Request** for request information or **Response** for response information. Both kinds of information contain links in blue that you can click for more information.

Use event log filters

You use event log filters to refine your searches through the event logs, including searches through event logs from multiple BIG-IP® devices.

1. Click **Monitoring** > **EVENTS** > **Web Application Security** > **Filters and Tags** > **Filters**.
2. To remove a filter, select the check box to the left of the filter and click **Remove**, then confirm the deletion in the dialog box that opens.
   The filter is removed from the Filters screen.
3. To modify a filter, click the name of the filter.
   The filter properties screen opens.
4. Review or revise the settings as needed.
   a) In the Query Expression area, review the current filter query, or type into the text box to modify it directly.

      In most cases, you will want to modify the query expression using the settings in the Query Parameters area, since that builds the query automatically, and so reduces the chance of error.

      The query has the format `method:'value' protocol:'value' severity:'value'`. For example: `method:'GET' protocol:'HTTPS' severity:'error'`.

   b) In the Query Parameters area, supply the parameter settings you want to be part of the filter.

      As you enter parameter settings, they are used to construct the filter query in the Query Expression area.

   c) Save your work.

   The filter is updated.

View and delete event log tags

You can review the tags defined for use with Web Application Security events and remove the tags.

1. Click **Monitoring** > **EVENTS** > **Web Application Security** > **Filters and Tags** > **Tags**.
   The Tags screen shows the defined tags.
2. To remove a tag, select the check box to the left of it and click **Remove**, then confirm the deletion in the dialog box that opens.
   The tag is removed from the Tags screen.

Determine DNS Sync Group Health

How do I check my sync group health?

Using the tools available on the BIG-IP® user interface, it can be difficult to determine the health of your DNS sync groups. When you use F5® BIG-IQ® Centralized Management to manage your DNS sync groups, the task becomes quite straightforward. You can do a quick health check, diagnose health issues, and even set up an alert to notify you if a sync group health issue occurs.

Check DNS sync group health

Before you can monitor the sync group health, you must add a BIG-IP® device configured in a DNS sync group to the BIG-IP Devices inventory list, and import the LTM® and DNS services.

When you use F5® BIG-IQ® Centralized Management to manage your DNS sync group, you can monitor the health status of the group. Sync group health relies on complete alignment of a variety of device configuration elements. Using BIG-IQ simplifies the process of determining the health of your DNS sync groups.

1. At the top of the screen, click **Devices**.
2. On the left, click **BIG-IQ CLUSTERS** > **DNS Sync Groups**.
   The screen displays the list of DNS sync groups defined on this device. A health indicator icon and a message describes the status of each group.
3. To view the general properties for a sync group, click the sync group name.

   Note: *For a list of Health Status error messages, refer to DNS sync group messages.*

   The screen displays the properties for the selected group. This screen shows an overview of your DNS sync group health. Under Status, you can see the current state (for example, `Required Services Down`, or `Health Check(s) Passed`) for each device in the group.
4. To view the health for an individual sync group member, click **Health** .
   The Health screen displays detailed information for each factor that contributes to the health of a DNS sync group. Following a definition of each factor, a Status row provides additional detail. For each indicator, the most serious issues impacting that indicator are listed first. Finally, if the status for a health indicator is not `Health Check(s) Passed`, the **Recommended Action** setting describes what you can do to correct the issue.
5. Resolve any reported issues on the managed devices, and then return to the DNS Sync Groups screen and click **Refresh Status**.
   Once you resolve all reported issues, the status for the DNS sync group changes to `Health Check(s) Passed`.

DNS sync group status messages

When BIG-IQ® Centralized Management completes health checks for a DNS sync group, an icon and a message display to indicate the current status. There are four icons, each with its own associated meaning.

Table 1: Health indicator icons

Icon	Meaning
🟩	Indicates that all health checks passed satisfactorily (green).

Icon	Meaning
◂	Indicates that the health status is unknown or uncertain (blue).
⚠	Indicates a warning, or that the group health is sub-optimal (yellow).
◆	Indicates that a critical issue was found (red).

Table 2: Health indicator messages

Message	Health indicator color	Description	Corrective Action
Awaiting Sync	Yellow	When considering the health of a DNS sync group, the single most important indicator of health is whether the devices in the sync-group have the same configuration in the master control program (MCP) daemon. *MCP* stores the configuration information for the BIG-IP® device. If the configuration is not the same (for devices in the sync group and MCP), then the devices could handle traffic differently, depending on what the configuration differences are.	Recommended Action: Wait a few minutes for synchronization to each member to occur. If synchronization does not complete, refer to troubleshooting solution. Related Solutions: SOL13690: Troubleshooting BIG-IP GTM synchronization and iQuery connections.
Certificate Expired	Red	BIG-IP DNS uses the device's Apache server certification to act as the server certification when establishing iQuery® connections. If this certificate expires, then all iQuery communication to and from this device is prevented. This indicator informs the DNS admin when one of the devices in a sync group has a device certificate that is near expiration, or is currently expired. This indicator only validates the expiration on the server certificate for each device. It does not examine the traffic certificates used in SSL profiles or DNSSEC certifications.	Renew the device certificate or import a new certificate. Related Solutions: SOL6353: Updating an SSL device certificate on a BIG-IP system.
Certificates Expiring	Yellow	The device certificate for this BIG-IP DNS device is near expiration. If the certificate expires, this BIG-IP DNS device will not be able to communicate with other BIG-IP devices using the iQuery protocol.	Either renew the device certificate or import a new certificate.
Changes Pending	Yellow	When considering the health of a DNS sync group, the single most important indicator of health is whether the devices	Recommended Action: Wait a few minutes for

Message	Health indicator color	Description	Corrective Action
		in the sync-group have the same configuration in the master control program (MCP) daemon. *MCP* stores the configuration information for the BIG-IP device. If the configuration is not the same (for devices in the sync group and MCP), then the devices could handle traffic differently, depending on what the configuration differences are.	synchronization to each member to occur. If synchronization does not complete, refer to troubleshooting solution. Related Solutions: SOL13690: Troubleshooting BIG-IP GTM synchronization and iQuery connections.
Collecting Data	Blue	Either the certificate has not yet been discovered by BIG-IQ or the device is unreachable.	If the certificate is the issue, the needed data should be collected automatically. If this condition persists, check the BIG-IQ logs for any error messages. If the device is unreachable, determine why BIG-IQ can not contact the BIG-IP device. There could be network issues, the device could be offline, or BIG-IQ Restjavad service could be is down.
Incompatible Device Versions	Red	A GTM sync group consists of one or more GTM devices. For sync to perform correctly, each device must have the same base version of TMOS installed. To determine the version of TMOS: view the version component of the output of `tmsh show sys version`.	Upgrade all BIG-IP devices in the sync group to the same version. Related Solutions: SOL8759: Displaying the BIG-IP Software Version. SOL13734: BIG-IP DNS synchronization group requirements.

Message	Health indicator color	Description	Corrective Action
Member Sync Disabled	Red	BIG-IP DNS devices have properties to control which sync group a device belongs to, and whether synchronization is enabled. A device can be a member of a sync group, but have synchronization disabled. Any changes made on a device on which synchronization is disabled cannot sync changes to the other devices. F5 recommends not having sync groups with synchronization disabled on some of the devices. We also recommend not making changes on devices if synchronization is disabled.	Enable synchronization on all devices in the group. Related Solutions: SOL13734: BIG-IP DNS synchronization group requirements.
Required Services Down	Red	For the BIG-IP DNS devices to be able to sync configuration changes, the following services (daemons) must be running on all the devices in the sync group: • `mcpd` • `gtmd` • `big3d` • `tmm` If any of these services is down, then configuration will not sync between the devices in the sync group. The sync group health is primarily concerned with reporting the health of only the sync group itself; not the health of the functionality provided by each device in the sync group.	Start stopped services Related Solutions: SOL13690: Troubleshooting BIG-IP DNS synchronization and iQuery connections Troubleshooting daemons.
Server Object Missing	Red	On the BIG-IP device, the DNS server objects define the IP address on which iQuery connections are made. There must be a server object for every DNS device in the sync group so that they can establish the necessary connections. This indicator validates that all devices have a server object, and that the necessary ports are open to allow the iQuery communication that happens over port 4353.	Verify that the DNS server objects have an associated self IP address. Related Solutions: SOL13734: BIG-IP DNS synchronization group requirements.
Syncing Changes	Yellow	When considering the health of a DNS sync group, the single most important indicator of health is whether the devices in the sync-group have the same configuration in the master control program (MCP) daemon. *MCP* stores the configuration information for the BIG-IP device. If the configuration is not the same (for devices in the sync group and MCP), then the devices could handle traffic	Recommended Action: Wait a few minutes for synchronization to each member to occur. If synchronization does not complete, refer to

Message	Health indicator color	Description	Corrective Action
		differently, depending on what the configuration differences are.	troubleshooting solution. Related Solutions: SOL13690: Troubleshooting BIG-IP GTM synchronization and iQuery connections.
Unknown Device Availability	Blue	The BIG-IQ device must collect data from each device in a sync group to be able to determine if the overall sync group is healthy. If BIG-IQ cannot reach one of the devices, then it cannot detect changes that make the overall group unhealthy. If a device cannot be reached, then the group is marked as unhealthy because there is no other way to know the health of the group.	Determine and fix loss of device availability. Related Solutions: SOL13690: Troubleshooting BIG-IP DNS synchronization and iQuery connections Troubleshooting daemons.
Unreachable Devices	Red	The BIG-IQ device must collect data from each device in a sync group to be able to determine if the overall sync group is healthy. If BIG-IQ cannot reach one of the devices, then it cannot detect changes that make the overall group unhealthy. If a device cannot be reached, then the group is marked as unhealthy because there is no other way to know the health of the group.	Determine and fix loss of device availability. Related Solutions: SOL13690: Troubleshooting BIG-IP DNS synchronization and iQuery connections Troubleshooting daemons.

How do I set up an alert for DNS sync group issues?

You can configure a BIG-IQ® SMTP alert to send email notifications when specific DNS sync group issues occur.

The following issues can trigger an alert:

- A new health status is generated for a DNS sync group. For instance, you might have just discovered a new sync group.
- The overall health status changes. For example, a device group that was healthy becomes unhealthy.
- The primary indicator (the most significant reason for the group's current health status) changed. (For example, the group is still unhealthy, but the reason is different than before.)

You enable or disable DNS alerts from the **System Management** > **Alerts** screen. For detailed instructions on creating an SMTP alert, refer to *How do I set up BIG-IQ to work with SMTP?* in the *F5 BIG-IQ Centralized Management: Licensing and Initial Setup* guide on `support.F5.com`.

Viewing GSLB Objects

View GSLB objects

Before you can view GSLB objects, you must discover and import BIG-IP® devices that are members of a DNS sync group that has GSLB objects.

When you use F5® BIG-IQ® Centralized Management to manage your DNS sync group, you can view the GSLB objects that are defined on devices in the sync group.

1. At the top of the screen, click **Configuration**.
2. On the left, click **DNS** > **GSLB**, and then select the object type that you want to view.
   The screen lists the objects that are defined on devices managed by this BIG-IQ system that match the object type you selected.. For each object (except topology records or topology regions) , icons indicate the health status and availability.
3. To view overview information about a particular object, select the check box for that object.
   The screen displays an overview area and a Related Items area for this object.
4. To see a list of related items for a GSLB object:
   a) Select the check box for that object.
   b) In the Related Items area, click **Show**.

      You can view the list of related items; and, for many of the items, you can click a link to view properties for that item.
5. To view the general properties for a GSLB object, click the name of that object.
   The properties screen for the selected object opens.

How do I manage permissions for DNS GSLB objects?

BIG-IQ® Centralized Management makes it straightforward for you to manage permissions that allow users to view global server load balancing (GSLB) objects only for the specific DNS GSLB objects you assign to them.

To provide permissions for a specific set of objects, you perform several tasks:

1. **Add a custom resource group** - In this task, you specify the GSLB objects that you want this user to work with. You create a resource group for each collection of objects that you want to assign to a user.
2. **Add a custom role** - Next, you associate the GSLB Viewer role type withthe resource groups that contain the objects you want your delegates to view. For example, if you had a resource group made up of two wide IPs, one named `SeattlePrime` and the other named `SeattleSecond` you might name this role `viewSeattle`.
3. **Add a custom user** - Finally, you create a user and assign a custom role to that user. The role gives that user permissions to view the objects that belong to the objects in the resource group. In the previous example, you could assign your custom user to the `viewSeattle` role to give that user the ability to view the GSLB objects in the two Seattle wide IPs.

For step by step guidance on each of these tasks, refer to the *Custom roles based on job responsibilities?* chapter in the *F5 BIG-IQ Centralized Management:Authentication, Roles, and User Management guide* on `support.f5.com`.

Troubleshooting using iHealth

What is iHealth?

The F5® iHealth® server is a tool that helps you troubleshoot potential issues. It does this by analyzing configuration, logs, command output, password security, license compliance, and so on.

From F5 BIG-IQ® Centralized Management, you can create a snapshot of a configuration in the form of a QKView file and then upload it to the F5 iHealth server. The file is compared to the iHealth database, which contains known issues, common configuration errors, and F5 published best practices. F5 returns an iHealth report you can use to identify any potential issues that you need to attend to.

How do I get access to send QKView files for my managed devices to the F5 iHealth diagnostics server?

You'll need a single sign on (SSO) to the F5® Support site to access the F5 iHealth® diagnostics server. If you don't have one yet, register at *https://login.f5.com/resource/login.jsp*

With access to the F5 iHealth diagnostics server you can upload QKView files and download iHealth reports for your managed devices.

1. At the top of the screen, click **Monitoring**.
2. On the left, click **REPORTS** > **Device** > **iHealth** > **Configuration**.
3. Click the **Add** button.
4. In the **Name** field, type a name to identify this user.
5. In the **Username** and **Password** fields, type this user's F5 Support SSO user name and password.
6. In the **Description** field, type an optional description for this user.
7. Click the **Test** button to verify you can reach the iHealth diagnostics site.
8. Click the **Save & Close** button at the bottom of the screen.

You can now upload QKView files to the F5 iHealth server to get iHealth reports for your managed devices.

Limit the number of simultaneous iHealth-related file transfers to and from BIG-IQ for my managed devices

If you want to limit how much traffic is dedicated to file activity related to iHealth® for your managed devices, you can specify the of simultaneous QKView file transfers to and from F5® BIG-IQ® Centralized Management.

1. At the top of the screen, click **Monitoring**.
2. On the left, click **REPORTS** > **Device** > **iHealth** > **Configuration**.
3. For the **QKView Transfer Limit** setting, click the **Edit** button.
4. In the **QKView Transfer Limit** field, type the greatest number of QKView files you want transferred to and from BIG-IQ at one time, per upload task.
5. Click the **Save & Close** button at the bottom of the screen.

Upload a QKView file to the F5 iHealth server to troubleshoot potential issues

To upload a QKView file, you must have access to the F5® iHealth® server configured on BIG-IQ® Centralized Management.

You upload a QKView file to F5 Networks to create an iHealth diagnostics report. You can use that report to troubleshoot potential issues with a managed device.

1. At the top of the screen, click **Monitoring**.
2. On the left, click **REPORTS** > **Device** > **iHealth** > **Tasks**.
3. Click the **QKView Upload** button.
4. In the **Name** field, type a name to identify this report, and type an optional identifier in the **Description** field.
5. If you have (and want to associate) a support case number with this QKView file, type that into the **F5 Support Case Number** field.

   This step is not required.
6. From the **Credential** list, select the credentials to log in to the iHealth diagnostic site.
7. From the **Available** list, click the device you want to upload a QKView file for.
8. Click the **Save & Close** button at the bottom of the screen.

When BIG-IQ finishes uploading the QKView file(s) to F5, it displays a status icon next to it on the Tasks screen.

If the upload fails, click the report's **Name** link and view the error message for more information. After F5 successfully receives the QKView file it creates an iHealth report. To view this report, go to the Device Reports screen.

Troubleshoot potential issues by viewing an iHealth device report

After you upload a QKView file for one or more BIG-IP® devices, the F5® iHealth® server returns a device report.

Review the device report so you can address any potential issues or vulnerabilities. From the report, you can access and sort heuristics associated with a device.

1. At the top of the screen, click **Monitoring**.
2. On the left, click **REPORTS** > **Device** > **iHealth** > **Device Reports**.
3. Click the **Open** link next to the report you want to view.
4. To sort the heuristics for a report you've opened, select an option from the **All Importance** and/or the **All Flags** list.
5. You can add a flag to a specific heuristic by selecting the check box next to it, and selecting a flag from the **All Flags** list.
6. To view more details about a specific heuristic, click on its link.
7. To view an article on the AskF5 Knowledge Center database to get more information about this heuristic, click the solution link.

Create a schedule to upload QKView files to the iHealth server

After you specify the credentials for a user to access the F5® iHealth® diagnostic server, you can create a QKView upload schedule.

Configuring BIG-IQ® Centralized Management to upload QKView files to the F5 iHealth diagnostic server on a regular basis means you'll get iHealth device diagnostics reports sent automatically to BIG-IQ for your BIG-IP devices. This information makes it easy for you to troubleshoot potential issues, and keeps you up-to-date about vulnerabilities that could cause security issues for your devices.

1. At the top of the screen, click **Monitoring**.
2. On the left, click **REPORTS** > **Device** > **iHealth** > **QKView Uploads Schedules**.
3. Near the top of the screen, click the **Create** button.

4. In the **Name** field, type a name to identify this report, and type an optional identifier in the **Description** field.
5. From the **Credential** list, select the credentials to log in to the iHealth diagnostic site.
6. From the **Upload Frequency** list, select how frequently you want to upload QKView files to the F5 iHealth server, and then select the day of the week or month.
7. Select a start date and time for this schedule.
8. Select an end date for this schedule, or select the **No End Date** check box.
9. From the **Available** list, select the device(s) you want to add to this schedule.
10. Click the **Save & Close** button at the bottom of the screen.

Now BIG-IQ will upload QKView files for the selected device on the schedule you specified.

Go to the Device Reports screen to view reports sent from the F5 iHealth server.

Create an upgrade advisor report before you upgrade BIG-IP system

Before you create an upgrade advisor report for a BIG-IP® system, you must specify the credentials for a user to access the F5® iHealth® diagnostic server, and upload the QKView file for that device to the F5 iHealth server.

Before upgrading, you create an upgrade advisor report so that you can prepare for any potential issues you might need to address.

1. At the top of the screen, click **Monitoring**.
2. On the left, click **REPORTS** > **Device** > **iHealth** > **Upgrade Advisor Report**.
3. Near the top of the screen, click the **Create** button.
4. From the **Device** list, select the device you want to run a report for.
5. From the **Target Version** list, select the version to which you are going to be upgrading this device.
6. In the **Name** and **Description** fields, type a name and an optional description for this task.
7. Click the **Save & Close** button at the bottom of the screen.

View the report on the Upgrade Advisor Reports screen and address any potential issues before you upgrade this BIG-IP device.

Legal Notices

Legal notices

Publication Date

This document was published on December 14, 2018.

Publication Number

MAN-0650-02

Copyright

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

Trademarks

For a current list of F5 trademarks and service marks, see *http://www.f5.com/about/guidelines-policies/trademarks*.

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

Patents

This product may be protected by one or more patents indicated at: *https://f5.com/about-us/policies/patents*.

Export Regulation Notice

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

RF Interference Warning

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

FCC Compliance

This equipment has been tested and found to comply with the limits for a Class A digital device pursuant to Part 15 of FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This unit generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case the user, at his own expense, will be required to take whatever measures may be required to correct the interference.

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

Canadian Regulatory Compliance

This Class A digital apparatus complies with Canadian ICES-003.

Standards Compliance

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

Index

A

- Access
  - remote logging
    - enabling *55*
- Access Reporting
  - managing specific user *41*
- Access reports
  - about *54*
  - about saving to CSV *39*
  - about setting up *39*
  - filtering *41*
  - for Access groups *39*
  - for all devices *39*
  - for clusters *39*
  - for discovered devices *39*
  - for unmanaged devices *39*
  - getting details from summaries *42*
  - limits *43*
  - saving to CSV *41*
  - session duration missing *44*
  - session termination missing *44*
  - setting the timeframe *43*
  - specifying the timeframe *41*
  - terminated session in Active report *44*
  - troubleshooting *54*
- active firewall policy
  - viewing *69*
- active firewall policy rules
  - properties *69*
- active sessions
  - stopping from Access *45*
- Active sessions report
  - using to stop active sessions *45*
- alert conditions
  - specifying *13*
- alerts
  - about *7*
  - about setting up SNMP v1 or 2 for sending *10*
  - configuring SMTP for *9*
  - for DSN sync group issues *83*
  - for system and deployment *12*
  - setting up conditions *13*
  - setting up SNMP Agent for sending *10*
  - setting up SNMP v1 or 2C for sending *12*
  - setting up SNMP version 3 Access *11*
- analytics
  - about *15*
- API (REST) audit log
  - about *37*
- application
  - creating for classification *63*
- application dashboard
  - for BIG-IQ *59*
- application monitoring
  - about analytics *15*
- application performance issues
  - analyzing *28*, *29*
- application summary
  - about *40*
  - dashboard *40*
- Application Summary dashboard
  - viewing *40*, *60*
- application tracking reporting *61*
- application visibility
  - about *40*
  - about classification presets *63*
  - about classification profiles *63*
  - and advanced configuration *61*
  - and memory allocation *65*
  - basic configuration *60*
  - creating a local traffic policy *62*
  - troubleshooting *65*
- applications
  - creating custom classification *64*
  - updating custom classification *63*
- archived audit logs
  - about *36*
- audit log
  - about REST API *37*
  - customizing display of *35*
  - filtering entries *33*
- audit log archive settings
  - managing *35*
- audit log display
  - customizing *35*
- audit log entries
  - filtering *33*
  - generation of *31*
  - properties of *32*
- audit log filtering
  - of entries *33*
- audit logs
  - about *31*
  - in high-availability configurations *37*
  - viewing differences *33*

B

- backups
  - alert for failure *7*
- BIG-IP communication
  - checking for data collection device *55*
- BIG-IP device troubleshooting
  - using iHealth *87*
- BIG-IP devices
  - stopping active sessions *45*
- BIG-IP logging profile
  - checking configuration *54*
- BIG-IP system
  - data collection device communication *55*
  - overview for configuring *59*
- BIG-IQ inventory
  - adding devices to *23*
- BIG-IQ system troubleshooting
  - using iHealth *87*

C

categories
  creating custom for classification *62*
centralized management
  of BIG-IP devices *23*
certificates
  alerts for expiration *7*
chart pane detail *17*
Classification
  creating profiles *64*
  updating profiles *63*
classification applications
  creating custom *64*
  updating custom *63*
classification categories
  creating custom *62*
classification signatures
  updating automatically *61*
  updating overview *60*
clock skew
  alert for *7*
cluster configuration
  checking for data collection device *54*
clusters
  for Access reporting *39*
CPU threshold
  alert for *7*

D

denied sessions
  about *46*
  viewing *46*
device availability
  specifying alerts for *13*
device discovery
  enabling statistics *23*
device groups availability
  specifying alerts for *13*
device statistics
  analyzing *27–29*
  browsing *27*
  enabling *23*
devices
  adding to BIG-IQ inventory *23*
  discovering *23*
diagnostics
  using iHealth for BIG-IP devices *87*
  using iHealth for BIG-IQ devices *87*
diagnostics for my managed devices
  using iHealth *87*
diagnostics report for managed devices
  uploading a QKView file *87*
differences
  in audit logs *33*
  viewing in audit logs *33*
dimensions pane detail *18*
directory usage
  specifying alerts for *13*
disk usage
  specifying alerts for *13*
DNS statistics
  overview screen *20*
DNS Sync Group
  health *79*
DNS sync group health
  checking *79*
  status messages *79*
DNS sync group issues
  setting up an alert *83*
DNS sync groups
  about checking health *79*
  checking health *79*
  health icons *79*
  setting up an alert *83*
DNS synch group
  alert for failure *7*
DNS traffic statistics
  analyzing *30*

E

Elasticsearch
  and upgrades *40*
email recipients
  configuring for alerts *12*
enabling statistics
  during discovery *23*
endpoint security check
  about *49*
endpoint software
  details *50*
  summary *49*
event logs
  about viewing for Web Application Security *77*
  using filters with Web Application Security *78*
  using tags with Web Application Security *78*
  viewing *77*
expired certificates
  alerting for *7*
expired licenses
  alerting for *7*

F

file transfers for iHealth files for managed devices
  to and from BIG-IQ for iHealth reports and QKView files *87*
firewall packet traces
  about *75*
firewall policy rules
  properties for active *69*
firewall rule
  about reports *73*
  creating reports *73*
  deleting reports *74*
firewall rule hit count *71*
firewall rule reports
  about *73*
  creating *73*
  deleting *74*
firewall rules
  monitoring *71*, *72*

framework health for device
- alert for *7*

G

GSLB object properties
- viewing *85*

GSLB objects
- about viewing *85*
- and how to manage permissions *85*
- viewing *85*

H

health
- about DNS sync groups *79*
- checking for DNS sync groups *79*
- specifying alerts for *13*
- status for DNS sync groups *79*

Health diagnostic reports for managed devices
- limiting number received simultaneously *87*

health indicator icons *79*

health indicator messages *79*

heuristics
- viewing for an iHealth report *88*

high resource usage
- looking for *27*

I

IdP assertion reports
- running *53*

IdP error reports
- running *54*

iHealth
- about *87*
- viewing a device report *88*

iHealth diagnostics service for managed devices
- getting and providing access to *87*

iHealth server
- creating a schedule to upload QKView files to *88*

L

licenses
- alerts for expiration *7*

load balancing issues
- determining *29*

local traffic policy
- creating for application visibility *62*

Logging Node
- unavailable, cause *44*
- unavailable, impact on Access reports *44*

logging profile
- checking data collection device *54*
- checking health *54*

M

memory health for device
- alert for *7*

monitoring
- firewall rules *71*, *72*

monitoring applications
- about analytics *15*

N

network access
- about *47*
- errors *48*
- performance *48*
- reconnect *48*
- reporting *47*
- usage *49*

network access summary
- view *47*

Network Security Reporting
- about *67*

notifications
- for system and deployment *12*

O

OAuth reports
- running *50*

OAuth server performance
- monitoring *51*

OAuth token summary
- monitoring *51*

P

packet traces
- about *75*
- creating *75*

performance
- OAuth server *51*

performance issues
- analyzing *29*

profiles
- creating Classification *64*
- updating Classification *63*

properties
- for active firewall policy rules *69*
- viewing for GSLB objects *85*

Q

QKView file uploads for managed devices
- limiting number sent simultaneously *87*

QKView files for managed devices
- uploading to F5 iHealth diagnostics service *87*

QKView uploads
- creating a schedule for *88*

R

reporting
- about elasticsearch *40*
- about upgrades *40*

Reporting screen

Reporting screen *(continued)*
- about *67*

reports
- creating for firewall rules *73*
- deleting for firewall rules *74*
- for firewall rules *73*
- running IdP assertions *53*
- running IdP errors *54*
- running OAuth *50*
- running SAML *51*
- running SP assertions *52*
- running SP errors *53*
- running SWG *45*

REST API audit log
- about *37*
- saving locally *37*

restjavad-audit.n.log
- about *37*

retention policy
- managing *25*

rules in active firewall policy
- viewing *69*

S

SAML reports
- running *51*

Secure Web Gateway Services reports, *See* SWG reports

security reporting
- about *67*

Session reports
- filtering *44*
- saving to CSV *44*
- specifying the timeframe *44*

shards
- resolve *56*
- unassigned *56*

signatures
- configuring updates *61*

SMTP
- about integration *7*
- configuring for alerts *9*
- specifying email recipients for alerts *12*

SNMP
- about integrating BIG-IQ Device *10*
- about integration *7*
- configuring version 1 and 2C for BIG-IQ *12*
- preparing to configure *10*
- specifying email recipients for alerts *12*

SNMP Agent
- configuring *10*

SNMP version 3 Access
- configuring *11*

software version health
- specifying alerts for *13*

SP assertion reports
- running *52*

SP error reports
- running *53*

SSL certificates
- about monitoring *13*

statistics

statistics *(continued)*
- enabling collection after discovery *24*
- enabling collection during device discovery *23*
- managing data retention policy *25*

statistics and graphs
- overview *15*

statistics collection
- enabling after discovery *24*
- enabling during device discovery *23*

statistics data
- managing retention policy *25*

statistics overview screen *16*

statistics overview screens *15*

statistics retention
- managing policy *25*

stats agent mismatched version
- alert for *7*

Stats agent mismatched version
- specifying alerts for *13*

Stats processing delay
- specifying alerts for *13*

summary
- OAuth token *51*

SWG reports
- about saving to CSV *39*
- about setting up *39*
- going from summaries to details *46*
- limits *43*
- running *45*
- setting the timeframe *43*

system alerts
- specifying *13*

system certificates
- about monitoring *13*

T

time control detail *16*

time controls *16*

traces
- creating *75*

traffic certificates
- about monitoring *13*

traffic intelligence
- creating a classification application *63*

traps
- for SNMP alerts *10*

troubleshooting
- creating a QKView upload schedule for *88*
- DNS traffic issues *30*
- for application visibility *65*
- for BIG-IP devices with iHealth *87*
- for BIG-IQ system with iHealth *87*
- using a device report *88*

troubleshooting for managed devices
- with iHealth QKView files *87*

troubleshooting issues for my managed devices
- using iHealth *87*

U

UCS backups

UCS backups *(continued)*
    alert for failure *7*
upgrade advisory report
    running for BIG-IP system *89*
upgrades
    run upgrade advisory report before upgrading BIG-IP system *89*
user visibility
    about *40*
    summary *40*

V

VDI
    about *47*
virtual desktop infrastructure*, See* VDI
virtual server
    and classification signatures *65*
    classification signatures *61*
    modifying *61*
    modifying for application visibility *65*
    simple *61*
    using advanced options *65*

W

Web Application Security event logs
    about viewing *77*
    using filters with *78*
    using tags with *78*
Web Application Security Reporting
    about *67*