BIG-IP® Analytics: Implementations

Version 13.1

Table of Contents

Setting Up Application Statistics Collection

What is Analytics?

Analytics, or Application Visibility and Reporting (AVR), is a module on the BIG-IP® system that you can use to visually analyze the performance of web applications, TCP traffic, DNS traffic, FastL4, and overall system statistics. The statistics are displayed in graphical charts where you can drill down into a specific time range or system aspect to better understand network performance on certain devices, IP addresses, memory and CPU utilization, and so on. You can further focus the statistics in the charts by selecting dimension entities such as applications or virtual servers.

For HTTP traffic, Analytics provides detailed metric values such as transactions per second, server and client latency, request and response throughput, and sessions. You can view these metrics for specific system dimensions such as: applications, virtual servers, pool members, transaction outcomes,URLs, specific countries, and additional detailed statistics about application traffic running through the BIG-IP system.

Transaction counters for response codes, user agents, HTTP methods, countries, and IP addresses provide statistical analysis of HTTP traffic that is going through the system. You can capture HTTP traffic for examination, and have the system send alerts so you can troubleshoot problems and immediately react to sudden changes.

For TCP and FastL4 traffic, reports show details about RTT (round trip time), goodput, connections, and packets. For TCP, you can also view statistics for delay analysis. Within these system dimensions, you can display information by the requests side, applications, virtual servers, remote host IP addresses, subnet addresses, next hops, countries, cities, continents, or user provided keys (from the TCP::analytics iRule). You can use the reports to gather information about TCP flows to better understand what is happening on your network. For example, you could view the charts by applications, then examine RTT averages, packet loss, and connection length to investigate user complaints about a slowdown.

You specify the type of traffic to monitor using different Analytics profiles. To view web application statistics, you use an *HTTP Analytics profile*, and to view TCP or FastL4 statistics, you use a *TCP Analytics profile*. Viewing system statistics does not require an Analytics profile.

Using remote logging capabilities with Analytics, your company can consolidate statistics gathered from multiple BIG-IP appliances onto syslog servers or SIEM devices, such as Splunk. A report scheduler allows you to periodically send email to users with specific types of reports that you design.

About HTTP Analytics profiles

An *HTTP Analytics profile* is a set of definitions that determines the circumstances under which the system gathers, logs, notifies, and graphically displays information regarding traffic to an application. You select an HTTP Analytics profile for each application you want to monitor. You associate the HTTP Analytics profile with one or more virtual servers used by the application. Each virtual server can have one HTTP and/or one TCP Analytics profile associated with it.

In the HTTP Analytics profile, you customize:

- What statistics to collect
- Where to collect data (locally, remotely, or both)
- Whether to capture the traffic itself
- Whether to send notifications

The BIG-IP® system includes a default HTTP Analytics profile called `analytics`. It serves as the parent of all other HTTP Analytics profiles that you create on the system. You can modify the default profile, or create custom HTTP Analytics profiles for each application if you want to track different data for each one. Certain settings, such as SMTP Configuration, Transaction Sampling, and the Subnets list, can only be set in the default HTTP Analytics profile.

Statistics > **Analytics** displays the HTTP Overview by default, which shows:

- Average transactions per second
- Average request throughput
- Average response throughput
- Average server latency
- Average page load time
- Average concurrent sessions
- Average new sessions

Charts shown on the HTTP Overview screen include the application data saved for all HTTP Analytics profiles associated with iApps application services and virtual servers on the system. You can filter the HTTP information by many different criteria, such as by application or URL. You can also drill down into the specifics on the charts, and use the options to further refine the information in the charts.

Overview: Collecting application statistics

This implementation describes how to set up the BIG-IP® system to collect application performance statistics. The system can collect application statistics locally, remotely, or both. You use these statistics for troubleshooting and improving application performance.

You can collect application statistics for one or more virtual servers or for an iApps® application service. If virtual servers are already configured, you can specify them when setting up statistics collection. If you want to collect statistics for an iApps application service, you should first set up statistics collection, creating an HTTP Analytics profile, and then create the application service.

The system can send alerts regarding the statistics when thresholds are exceeded, and when they cross back into the normal range. You can customize the threshold values for transactions per second, latency, page load time, and throughput.

Task Summary

Customizing the default HTTP Analytics profile
Collecting application statistics locally
Collecting application statistics remotely
Getting application performance alerts
Creating an SMTP server configuration

Customizing the default HTTP Analytics profile

The Application Visibility and Reporting (AVR) module includes a default HTTP Analytics profile called `analytics`. You can edit the settings in the default profile so it uses the values you want.

Certain information can be specified only in the default HTTP Analytics profile: the SMTP configuration (a link to an SMTP server), transaction sampling (whether enabled or not), and subnets (assigning names to be used in the reports). To edit these values, you need to open and edit the default profile.

1. On the Main tab, click **Local Traffic** > **Profiles** > **Analytics** > **HTTP Analytics**.

Tip: *To have the **Analytics** listed, you need to provision Application Visibility and Reporting (AVR) first.*

The **Profiles: Analytics** screen opens.

2. Click the profile called **analytics**.
   The configuration screen for the default HTTP Analytics profile opens.
3. For the **Statistics Logging Type** setting, verify that **Internal** is selected. If it is not, select it.

   Selecting **Internal** causes the system to store statistics locally, and you can view the charts on the system by starting at the Main tab, and clicking **Statistics** > **Analytics**.
4. To send email alerts, specify an **SMTP Configuration**.

   You can change the SMTP configuration only in the default profile. It is used globally for the system. If no configuration is available, click **Create** to create one.
5. For the **Notification Type** setting, select how you want the system to send alerts and notifications.

Option	Description
Syslog	Select **Syslog** if you want the system to send notification and alert messages to the local log system. You can view the messages on the **System** > **Logs** > **Local Traffic** screen.
SNMP	Select **SNMP** if you want the system to send notification and alert messages as SNMP traps. You can create the trap by clicking **Configuration can be found here** (**System** > **SNMP** > **Traps** > **Destination**). Enabling SNMP automatically sets up Syslog notifications, too.
E-mail	Select **E-mail** if you want the system to send notification and alert messages to email addresses. Type each email address in the **Notification E-Mails** field, and click **Add** to create the list. This option requires that the default analytics profile includes an SMTP configuration.

   When you select a notification type, the screen displays the Alerts and Notifications Configuration area, where you can indicate the criteria for alerts and notifications.
6. If you want the system to perform traffic sampling, make sure that for **Transaction Sampling**, the **Sample** check box is selected.

   You can change this setting only in the default profile.

Tip: *Sampling improves system performance. F5 recommends that you enable sampling if you generally use more than 50 percent of the system CPU resources, or if you have at least 100 transactions in 5 minutes for each entity.*

7. If you want the system to collect and display statistics, according to the expressions written in an iRule, select the **Publish iRule Statistics** check box.

   The iRule statistics can be viewed per Analytics profile on the command line by typing `ISTATS dump`.

Important: *For the system to collect iRule statistics, you must also write an iRule describing which statistics the system should collect.*

8. In the Associated Virtual Servers area, specify the virtual servers for which to capture application statistics:
   a) For the **Virtual Servers** setting, click **Add**.
   b) From the Select Virtual Server popup that displays, select the virtual servers to include and then click **Done**.

Note: *Only virtual servers previously configured with an HTTP profile display in the list (because the data being collected applies to HTTP traffic). Also, you can assign only one HTTP Analytics profile to a virtual server; therefore, the list displays only virtual servers that have not been assigned an Analytics profile.*

Special considerations apply if using Analytics on a BIG-IP system with both Application Security Manager™ and Access Policy Manager®, where security settings (in Portal Access webtop or an iRule) redirect traffic from one virtual server to another. In this case, you need to attach the HTTP Analytics profile to the second virtual server to ensure that the charts show accurate statistics.

9. In the Statistics Gathering Configuration area, for **Collected Metrics**, select additional statistics you want the system to collect from the requests:

Option	Description
Max TPS and Throughput	Collects statistics showing the maximum number of transactions occurring per second and the amount of traffic moving through the system (maximum request and response throughput is collected and recorded separately).
Page Load Time	Tracks how long it takes an application user to get a complete response from the application, including network latency and completed page processing. ***Note:*** *End-user response times and latencies can vary significantly based on geography and connection types.*
User Sessions	Stores the number of unique user sessions. For **Timeout**, select the number of minutes of user inactivity to allow before the system considers the session to be over. For **Cookie Secure Attribute**, specify whether to secure session cookies. Options are **Always**, the secure attribute is always added to the session cookie; **Never**, the secure attribute is never added to the session cookie; or **Only SSL**, the secure attribute is added to the session cookie only when the virtual server has a client SSL profile (the default value).

By default, the system collects many metrics, including TPS, throughput, server latency, response time, network latency, and so on. You can select the ones here in addition to the ones already collected once the Analytics profile is attached to one or more virtual servers.

10. In the Statistics Gathering Configuration area, for **Collected Entities**, select additional entities to collect statistics for each request.

Option	Description
URLs	Collects the requested URLs.
Countries	Saves the name of the country where the request came from, and is based on the client IP address criteria.
Client IP Addresses	Saves the IP address where the request originated. The address saved also depends on whether the request has an XFF (X-forwarded-for) header and whether the HTTP profile accepts XFF headers.
Client Subnets	Saves statistics for predefined client subnets. Client subnets can be added in the Subnets area of the default HTTP Analytics profile.
Response Codes	Saves HTTP response codes that the server returned to requesters.
User Agents	Saves information about browsers making the request.
Methods	Saves HTTP methods in requests.

By default, the system collects many entity statistics, including virtual servers, pool members, browser names, operating system, and so on. You can select the ones here in addition to the ones already collected once the Analytics profile is attached to one or more virtual servers.

11. If you are collecting statistics for Client Subnets, you can name the subnets so the reports show a name (such as a department name) instead of an IP address. To do this, add the subnets:
    a) For the **Add New Subnet** setting **Name** field, type the name to use, and in the **Mask** field, type the IP address of the subnet.
    b) Click **Add**.

    The subnets are added to the list of Active Subnets. If displaying relevant data, the names of the subnets appear in the Analytics statistics.
12. Click **Update** to save your changes.

Statistics are collected for traffic going to the virtual servers specified in this profile.

You can create new HTTP Analytics profiles if you need to. New Analytics profiles inherit their values from the default Analytics profile. You can modify the values in the new profiles (except the ones that are set only in the default profile such as SMTP configuration). For example, you might want to send reports about two different applications to different managers. So you could have different emails listed in the notification type settings in two Analytics profiles.

Collecting application statistics locally

You need to provision the Application Visibility and Reporting (AVR) module before you can collect application statistics locally.

You can configure the BIG-IP® system to collect specific application statistics locally.

1. On the Main tab, click **Local Traffic** > **Profiles** > **Analytics** > **HTTP Analytics**.

   Tip: *If **Analytics** is not listed, this indicates that Application Visibility and Reporting (AVR) is not provisioned, or you do not have rights to create profiles.*

   The HTTP Analytics screen opens.
2. Click **Create**.
   The New HTTP Analytics profile screen opens.
3. In the **Profile Name** field, type a unique name for the Analytics profile.
4. From the **Parent Profile** list, select the profile from which you want to inherit settings.

   The default profile is often used as the parent profile.

   The new profile inherits the values from the parent profile. If the parent is changed, the inherited values in the new profile also change.
5. Select the **Custom** check box.
6. For the **Statistics Logging Type** setting, verify that **Internal** is selected. If it is not, select it.

   Selecting **Internal** causes the system to store statistics locally, and you can view the charts on the system by starting at the Main tab, and clicking **Statistics** > **Analytics**.
7. You can use the default values for the rest of the General Configuration settings.
8. In the Associated Virtual Servers area, specify the virtual servers for which to capture application statistics:
    a) For the **Virtual Servers** setting, click **Add**.
    b) From the Select Virtual Server popup that displays, select the virtual servers to include and then click **Done**.

Note: *Only virtual servers previously configured with an HTTP profile display in the list (because the data being collected applies to HTTP traffic). Also, you can assign only one HTTP Analytics profile to a virtual server; therefore, the list displays only virtual servers that have not been assigned an Analytics profile.*

Special considerations apply if using Analytics on a BIG-IP system with both Application Security Manager™ and Access Policy Manager®, where security settings (in Portal Access webtop or an iRule) redirect traffic from one virtual server to another. In this case, you need to attach the HTTP Analytics profile to the second virtual server to ensure that the charts show accurate statistics.

9. In the Statistics Gathering Configuration area, select the **Custom** check box.
10. In the Statistics Gathering Configuration area, for **Collected Metrics**, select additional statistics you want the system to collect from the requests:

Option	Description
Max TPS and Throughput	Collects statistics showing the maximum number of transactions occurring per second and the amount of traffic moving through the system (maximum request and response throughput is collected and recorded separately).
Page Load Time	Tracks how long it takes an application user to get a complete response from the application, including network latency and completed page processing. ***Note:*** *End-user response times and latencies can vary significantly based on geography and connection types.*
User Sessions	Stores the number of unique user sessions. For **Timeout**, select the number of minutes of user inactivity to allow before the system considers the session to be over. For **Cookie Secure Attribute**, specify whether to secure session cookies. Options are **Always**, the secure attribute is always added to the session cookie; **Never**, the secure attribute is never added to the session cookie; or **Only SSL**, the secure attribute is added to the session cookie only when the virtual server has a client SSL profile (the default value).

By default, the system collects many metrics, including TPS, throughput, server latency, response time, network latency, and so on. You can select the ones here in addition to the ones already collected once the Analytics profile is attached to one or more virtual servers.

11. In the Statistics Gathering Configuration area, for **Collected Entities**, select additional entities to collect statistics for each request.

Option	Description
URLs	Collects the requested URLs.
Countries	Saves the name of the country where the request came from, and is based on the client IP address criteria.
Client IP Addresses	Saves the IP address where the request originated. The address saved also depends on whether the request has an XFF (X-forwarded-for) header and whether the HTTP profile accepts XFF headers.
Client Subnets	Saves statistics for predefined client subnets. Client subnets can be added in the Subnets area of the default HTTP Analytics profile.
Response Codes	Saves HTTP response codes that the server returned to requesters.
User Agents	Saves information about browsers making the request.

Option	Description
Methods	Saves HTTP methods in requests.

By default, the system collects many entity statistics, including virtual servers, pool members, browser names, operating system, and so on. You can select the ones here in addition to the ones already collected once the Analytics profile is attached to one or more virtual servers.

12. Click **Finished**.

The BIG-IP system collects the statistics specified in the Analytics profile. You can view the statistics by clicking **Statistics** > **Analytics**.

Collecting application statistics remotely

You need to provision the Application Visibility and Reporting (AVR) module before you can collect application statistics remotely. To specify where the BIG-IP® system sends log messages remotely, you must have set up logging and created a publisher.

You can configure the BIG-IP system to collect application statistics and store them remotely on Syslog servers or SIEM devices, such as Splunk.

1. On the Main tab, click **Local Traffic** > **Profiles** > **Analytics** > **HTTP Analytics**.

   Tip: *If **Analytics** is not listed, this indicates that Application Visibility and Reporting (AVR) is not provisioned, or you do not have rights to create profiles.*

   The HTTP Analytics screen opens.
2. Click **Create**.
   The New HTTP Analytics profile screen opens.
3. In the **Profile Name** field, type a unique name for the Analytics profile.
4. Select the **Custom** check box.
5. For the **Statistics Logging Type** setting, select the **External** check box.

   Unless you want to view statistics locally, too, you can clear the **Internal** check box.

   The **Remote Publisher** setting displays, below the **Traffic Capturing Logging Type** setting.
6. If you want the system to capture traffic, for the **Traffic Capturing Logging Type** setting, specify whether to store the traffic locally or on a remote server.

Option	Description
Internal	Specifies that the system captures a portion of traffic and stores it locally. You can view the captured data on the **System** > **Logs** > **Captured Transactions** screen.
External	Specifies that the system captures a portion of traffic and stores it on a remote server.

   When you select the traffic capturing logging type, the screen displays the Capture Filter area, where you can indicate exactly what information to sample and log.
7. From the **Remote Publisher** list, select the publisher that includes the destination to which you want to send log messages.

   Tip: *Refer to External Monitoring of BIG-IP® Systems: Implementations for details.*
8. If you want the system to send email notifications, review the **SMTP Configuration** field to ensure that a configuration is specified and not the value **None**.

   You can configure SMTP only in the default Analytics profile. If it is not configured, you can save the profile and edit the default profile where you can select an existing SMTP configuration or create a

new one. (If you click the **analytics** link without saving the new profile you are working on, you will lose the unsaved changes.)

9. For the **Notification Type** setting, select how you want the system to send alerts and notifications.

Option	Description
Syslog	Select **Syslog** if you want the system to send notification and alert messages to the local log system. You can view the messages on the **System** > **Logs** > **Local Traffic** screen.
SNMP	Select **SNMP** if you want the system to send notification and alert messages as SNMP traps. You can create the trap by clicking **Configuration can be found here** (**System** > **SNMP** > **Traps** > **Destination**). Enabling SNMP automatically sets up Syslog notifications, too.
E-mail	Select **E-mail** if you want the system to send notification and alert messages to email addresses. Type each email address in the **Notification E-Mails** field, and click **Add** to create the list. This option requires that the default analytics profile includes an SMTP configuration.

   When you select a notification type, the screen displays the Alerts and Notifications Configuration area, where you can indicate the criteria for alerts and notifications.

10. In the Associated Virtual Servers area, specify the virtual servers for which to capture application statistics:
    a) For the **Virtual Servers** setting, click **Add**.
    b) From the Select Virtual Server popup that displays, select the virtual servers to include and then click **Done**.

Note: *Only virtual servers previously configured with an HTTP profile display in the list (because the data being collected applies to HTTP traffic). Also, you can assign only one HTTP Analytics profile to a virtual server; therefore, the list displays only virtual servers that have not been assigned an Analytics profile.*

   Special considerations apply if using Analytics on a BIG-IP system with both Application Security Manager™ and Access Policy Manager®, where security settings (in Portal Access webtop or an iRule) redirect traffic from one virtual server to another. In this case, you need to attach the HTTP Analytics profile to the second virtual server to ensure that the charts show accurate statistics.

11. In the Statistics Gathering Configuration area, for **Collected Metrics**, select additional statistics you want the system to collect from the requests:

Option	Description
Max TPS and Throughput	Collects statistics showing the maximum number of transactions occurring per second and the amount of traffic moving through the system (maximum request and response throughput is collected and recorded separately).
Page Load Time	Tracks how long it takes an application user to get a complete response from the application, including network latency and completed page processing. ***Note:*** *End-user response times and latencies can vary significantly based on geography and connection types.*
User Sessions	Stores the number of unique user sessions. For **Timeout**, select the number of minutes of user inactivity to allow before the system considers the session to be over. For **Cookie Secure Attribute**, specify whether to secure session cookies. Options are **Always**, the secure attribute is always added to the session cookie; **Never**, the secure attribute is never added to the session cookie; or **Only SSL**,

Option	Description
	the secure attribute is added to the session cookie only when the virtual server has a client SSL profile (the default value).

By default, the system collects many metrics, including TPS, throughput, server latency, response time, network latency, and so on. You can select the ones here in addition to the ones already collected once the Analytics profile is attached to one or more virtual servers.

12. In the Statistics Gathering Configuration area, for **Collected Entities**, select additional entities to collect statistics for each request.

Option	Description
URLs	Collects the requested URLs.
Countries	Saves the name of the country where the request came from, and is based on the client IP address criteria.
Client IP Addresses	Saves the IP address where the request originated. The address saved also depends on whether the request has an XFF (X-forwarded-for) header and whether the HTTP profile accepts XFF headers.
Client Subnets	Saves statistics for predefined client subnets. Client subnets can be added in the Subnets area of the default HTTP Analytics profile.
Response Codes	Saves HTTP response codes that the server returned to requesters.
User Agents	Saves information about browsers making the request.
Methods	Saves HTTP methods in requests.

By default, the system collects many entity statistics, including virtual servers, pool members, browser names, operating system, and so on. You can select the ones here in addition to the ones already collected once the Analytics profile is attached to one or more virtual servers.

13. If one of the **Traffic Capturing Logging Type** check boxes is selected, in the Capture Filter area, adjust the settings to specify criteria to determine what application traffic to capture.

Tip: *You can use the captured information for troubleshooting purposes.*

14. Click **Finished**.

The BIG-IP system collects statistics regarding application traffic described by the Analytics profile and stores the statistics on a separate remote management system, where you can view the information.

Getting application performance alerts

Before you can configure the system to send alerts concerning statistics, you need to have created an Analytics profile to collect application statistics locally (**Statistics Logging Type** must have **Internal** selected). To set up email alerts, the default **analytics** profile must specify an SMTP configuration.

You can configure the BIG-IP® system to send alerts concerning local application statistics based on threshold values that you set. The system sends notifications when threshold values are breached, and when they return to normal. Therefore, it is a good idea to get familiar with the typical statistics for the web application before attempting to set up alerts and notifications. When you understand the typical values, you can configure the system to alert you of limiting system situations, such as system overload.

Note: *End user response times and latencies can vary significantly based on geography and connection types, which makes it difficult to set an accurate alerting threshold for page load times.*

1. On the Main tab, click **Local Traffic** > **Profiles** > **Analytics** > **HTTP Analytics**.

Tip: *To have the **Analytics** listed, you need to provision Application Visibility and Reporting (AVR) first.*

The **Profiles: Analytics** screen opens.

2. Click the name of a previously created Analytics profile, or create a new one.
3. Select the **Custom** check box.
4. For the **Statistics Logging Type** setting, verify that **Internal** is selected. If it is not, select it.

   Selecting **Internal** causes the system to store statistics locally, and you can view the charts on the system by starting at the Main tab, and clicking **Statistics** > **Analytics**.
5. To send email alerts, specify an **SMTP Configuration** (this can only be done on the default **analytics** profile).

   If you created a new profile, configure SMTP later.
6. For the **Notification Type** setting, select how you want the system to send alerts and notifications.

Option	Description
Syslog	Select **Syslog** if you want the system to send notification and alert messages to the local log system. You can view the messages on the **System** > **Logs** > **Local Traffic** screen.
SNMP	Select **SNMP** if you want the system to send notification and alert messages as SNMP traps. You can create the trap by clicking **Configuration can be found here** (**System** > **SNMP** > **Traps** > **Destination**). Enabling SNMP automatically sets up Syslog notifications, too.
E-mail	Select **E-mail** if you want the system to send notification and alert messages to email addresses. Type each email address in the **Notification E-Mails** field, and click **Add** to create the list. This option requires that the default analytics profile includes an SMTP configuration.

   When you select a notification type, the screen displays the Alerts and Notifications Configuration area, where you can indicate the criteria for alerts and notifications.
7. In the Alerts and Notifications Configuration area, for the **Add New Rule** setting, define the rules that determine when the system sends alerts. Note that you cannot add overlapping rules, for example, two rules that request an alert when average TPS is greater than **100** and greater than **50** for **200** seconds.
   a) For **Alert when**, select the condition under which you want to send an alert.
   b) Select **below** or **above**, type an integer that represents the threshold value, and type the number of seconds (an integer, `300` or greater,) during which the rule has to apply.
   c) Select the granularity level to which the threshold applies: traffic sent to an **Application**, a **Virtual Server**, or a **Pool Member**.
   d) Click **Add**.
   The rule is added to the list of Active Rules.

   Continue to add as many rules as you want to specify conditions under which you want to be alerted.
8. Click **Update**.
9. If SNMP is not configured on the BIG-IP system and you want to send SNMP traps, configure it now:
   a) In the General Configuration area, for the **Notification Type** setting, next to **SNMP**, click the link. The SNMP Traps Destination screen opens.
   b) Click **Create**.
   c) Configure the version, community name, destination IP address, and port.
   d) Click **Finished**.
10. If you need to configure SMTP (if sending alerts by email), click the default **analytics** profile on the Profiles: Analytics screen.
    a) For **SMTP Configuration**, select an existing configuration.

b) If no SMTP configurations are listed, click the **here** link to create one. When you are done, you need to select the configuration you created in the default **analytics** profile.

Based on the rules you configured and the notification type, the system sends an alert when thresholds are breached and when they cross back from the threshold.

Creating an SMTP server configuration

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

1. On the Main tab, click **System** > **Configuration** > **Device** > **SMTP**.
2. Click the **Create** button.
   The New SMTP Configuration screen opens.
3. In the **Name** field, type a name for the SMTP server that you are creating.
4. In the **SMTP Server Host Name** field, type the fully qualified domain name for the SMTP server host.
5. In the **SMTP Server Port Number** field, type a port number.

   For no encryption or TLS encryption, the default is `25`. For SSL encryption, the default is `465`.
6. In the **Local Host Name** field, type the host name used in the SMTP headers in the form of a fully qualified domain name.

   This host name is not the same as the BIG-IP® system's host name.
7. In the **From Address** field, type the email address that you want displayed as the reply-to address for the email.
8. From the **Encrypted Connection** list, select the encryption level required for the SMTP server.
9. To require that the SMTP server validates users before allowing them to send email, select the **Use Authentication** check box, and type the user name and password required to validate the user.
10. Click the **Finish** button.

You can now configure the system to use this SMTP server to send emails. For the SMTP mailer to work, you must make sure the SMTP server is on the DNS lookup server list, and configure the DNS server on the BIG-IP® system.

Examining and Exporting Application Statistics

Overview: Examining and exporting application statistics

This implementation describes how to view application statistics on the BIG-IP® system. It describes how you can examine the statistics in the Analytics charts when Application Visibility and Reporting (AVR) is provisioned. Analytics charts display statistical information about traffic on your system. The system updates the information every five minutes.

The Overview screen shows all of the HTTP statistics in one place, including averages for transactions per second (TPS), request and response throughput, server latency, page load time, concurrent sessions, and new sessions. You can filter, drill down, and view selected information by different metrics, such as by application, virtual server, URL, country, and so on.

The Analytics Custom screen provides a summary of the most frequent recent types of application traffic, such as the most accessed virtual servers, URLs, pool members, and so on. You can design the Analytics Custom screen so that it shows the specific types of data you are interested in.

You can schedule the reports to be sent to email addresses periodically. From any of the displayed reports, you can also export them to a PDF file, or send the report to one or more email addresses.

Note: *The displayed Analytics statistics are rounded up to two digits.*

Examining application statistics

Before you can look at the application statistics, you need to have created an HTTP Analytics profile so that the system is capturing the application statistics internally on the BIG-IP® system. You must associate the Analytics profile with one or more virtual servers (in the HTTP Analytics profile or in the virtual server). If you created an iApp application service, you can use the provided template to associate the virtual server.

You can review, filter, and compare HTTP statistics for traffic on the BIG-IP system. The HTTP Overview screen provides visibility into application behavior, user experience and client activity, transactions, data center resource usage, and more.

1. On the Main tab, click **Statistics** > **Analytics** > **HTTP**.
   The Overview screen opens and displays current HTTP statistics averaged over the last hour. On the screen, you can see time controls on the top, charts on the left, and a list of dimensions on the right.
2. Use the time settings at the top of the screen to set a time range or refresh the information on screen.
   To immediately update the statistics on screen, adjust the time range or refresh settings.

Time Focus	Select the time range of the displayed data. ***Note:*** *Additional time options become available as your system gathers more data.*
Currently Selected Time Range	Displays the current time range of the displayed data.
Auto-Refresh Interval Selector	Select how frequently the data on this screen is refreshed.
Manual Refresh	Click **Refresh** to trigger an immediate refresh of the displayed data.

Manual Time Adjustment Handles	Set the data to a specific window of time within the currently selected time range. Use the handles at either end of the time line to define the specific time you want to examine. Use the handle above the time line to display data that is outside the selected time range.

Note: *Adjusting the time range to display previous data stops the auto-refresh so you can focus on a specific data point.*

You can zoom into a specific time range within a chart. Select an area within the chart and then click the magnifying glass icon.

Note: *Selecting a time range within the chart stops the screen's auto-refresh settings.*

3. Review the HTTP Activity area for application traffic activity, and to evaluate your system's traffic performance.
   - Use the Transaction Outcomes (Average TPS) chart to analyze the outcome assigned by the BIG-IP system to the application request and response exchange.
   - Use the Avg Throughput (bps) chart to determine the average number of bytes per second processed by the BIG-IP system during application requests and responses.
   - Use the Server Latency (ms) chart to determine the time required for a server response once the BIG-IP system sends a request.
   - Use the Page Load Time (ms) chart to determine the time required for a client to receive a server response after sending a request via the BIG-IP system.
4. Review the Virtual Server Activity area to evaluate the traffic processing performance of each virtual server.

Important: *Selecting a single virtual server displays the charts in the panel. Ensure that you have cleared all other filters when selecting a virtual server.*

   - Use the Avg & Max TPS (tps) chart to evaluate the highest and median transaction processing per second for your selected virtual server.
   - Use the Max Throughput (bps) chart to evaluate the maximum number of bytes per request or response that was processed by the selected virtual server.
   - Use the Concurrent User Sessions chart to evaluate the average number of concurrent session that were open at the same time for the selected virtual server.

You can continue to review system statistics on the entire system. As a result, you become more familiar with the system, applications, resource utilization, and more. You can focus on the specific data you need using the filters and comparison chart option provided in the Dimensions pane.

You can save the statistics in a file, and send the file to select users by email. You can also set up schedules to send specific reports to specific users (go to the Scheduled Reports screen, **Analytics** > **Scheduled Reports**).

Filter statistics data using the Dimensions pane

By default, the charts and dimensions tables display unfiltered data that is relevant to all monitored BIG-IP® system aspects. You can filter the displayed data by selecting entities within dimensions in the Dimensions pane.

Important: *Applying filters in the Dimensions pane updates all statistics displayed on screen with data that corresponds to your selection.*

1. On the Main tab, click **Statistics** > **Analytics** > **HTTP**.
2. Locate the Dimensions pane on the right side of the screen.

3. Review data according to pre-configured device group, and filter the displayed data according to a specific configuration by selecting an option from **Device Group**.
4. Review dimension entities and their statistics in table form by expanding a dimension widget. To filter by dimension entities, select one or more entities from that dimension.

   For example: You can filter by selecting individual Virtual Servers or Applications to display statistics in the charts that are specific to your selection. You can select entities from multiple dimensions that have corresponding data.
5. You can adjust the table view by selecting the Dimensions pane handle and dragging it to the left side of the screen.

   Tip: *You can expand the pane to full screen view by double-clicking the Dimensions pane handle.*
6. Clear all filter selections or those for a dimension:
   - To clear all selections, click the gear icon at the top of the Dimensions pane and select **Clear All**.
   - To clear selections for a dimension, click the options icon (three horizontal lines to the left of the title), and select **Clear Selection**.

About comparison charts

The AVR charts display aggregated statistics for your entire BIG-IP® system. You can create customized charts based on specific, compatible data of interest, with a comparison chart. You create comparison charts using dimension entities to highlight specific data metrics, or to compare multiple entities in one chart.

Create a comparison chart using the Dimensions pane

You can create new charts that present statistic information about your BIG-IP® system for selected entities from a dimension in the Dimensions pane. Once a new chart is created, you can adjust the metric value that is presented. You can create multiple comparison charts per screen.

1. On the Main tab, click **Statistics** > **Analytics** > **HTTP**.
2. In the Dimensions pane, expand a dimension widget to view its entity list.
3. Select one or more dimension entities for the comparison chart by clicking the entity title. You can also select entities in other dimensions that have compatible data.

   Note: *Selecting entities automatically filters information in the Charts pane and compatible data in other dimensions. You can remove these filters once the comparison chart is created.*
4. Click the dimension's menu icon and select **Add Comparison Chart**.

   Tip: *You can right click one of the selected entities to view the dimension widget menu.*

   A comparison chart displays in the Charts pane.
5. Adjust the displayed metric unit by selecting a different metric from the list next to the comparison chart title.

   By default, the chart displays data by the selected Sort By metric for the entity's dimension.

   Note: *Comparison charts persist in the Charts pane until they are removed. You can remove a comparison chart by selecting the* ***X*** *icon in the top right corner of the chart.*

The new comparison chart displays data for the selected entities in the Charts pane over the selected time period.

About the reporting interval for charts and reports

The system updates the statistics for charts and reports at five minute intervals: at five minutes after the hour, ten minutes after the hour, and so on. Each five-minute mark includes data from the previous five minutes; so 12:45 includes data starting from 12:40:01 to 12:45:00.

Charts and data that you export from charts reflect the publishing interval of five minutes. For example, if you request data for the time period 12:40-13:40, the data in the chart or in the file that you export is for that time period. But if there is a request for data from 12:42-13:42, the data in the chart is from 12:45-13:45. By default, the BIG-IP® system displays one hour of data.

Saving or emailing report files

To send reports by email, the default `analytics` profile must specify an SMTP configuration (**Local Traffic** > **Profiles** > **Analytics**).

You can export or email any of the Analytics charts including those which display statistics for HTTP, TCP, memory, disk, virtual servers, and other charts available on your system.

1. On the main tab, click **Statistics** > **Analytics** and select the type of chart to display.
2. Adjust the chart so that it shows the information you want, adjusting the content as needed.
3. On the upper right of the charts screen, click **Export**.

   Tip: *To send the report to others by email, go to* ***Statistics*** > ***Analytics*** > ***Scheduled Reports****.*
4. Click **Export**.

Customizing your statistics view

Before you can view HTTP application statistics, you need to have created an Analytics profile so that the system is capturing the application statistics internally on the BIG-IP® system. You must associate the Analytics profile with one or more virtual servers (in the Analytics profile or in the virtual server). If you created an iApp application service, you can use the provided template to associate the virtual server.

You can customize how you view statistics by displaying the information you want, organized as you want to see it into data-specific *widgets*. A set of default widgets is provided showing HTTP statistics for the top URLs, pool members, virtual servers, client subnets, and countries. You can create additional widgets or reorganize what's there.

1. On the Main tab, click **Statistics** > **Analytics** > **HTTP** > **Custom Page**.
   The Custom Page opens showing current HTTP statistics. By default, there are five widgets organized in two columns.
2. To view statistics for a particular device group, from the **Device Group** list, select the one you want.
3. To adjust the time range for all widgets, from **Override time range to**, select a new time frame for which to view statistics.

   If you select **(per widget)**, you can specify different time ranges for each widget.
4. For each widget you want to change, click the gear icon and select **Settings**.
   The Modify Widget Properties popup opens where you can change what the widget shows and the format used.
5. To change the order of the widgets, drag them up or down within the column.
6. To delete a widget if you do not need that information, click the gear icon and select **Delete**.
7. To focus in on the specific details you want more information about in any widget, click an item in the chart.
   The system refreshes the charts and displays information about the item. Click Back to return to the Custom Page.

8. To create a new widget in either column, click **Add Widget** at the bottom of the column.
   a) Fill in the Add New Widget popup screen to define the widget.
   b) From the **Available Measurements**, select the measurement to use.
   c) If there is a choice, select the data visualization.
   d) Click **Done**.

   The new widget displays in the column.
9. Click **Export** to create a report of this information.

Note: *The timestamp on the report reflects a publishing interval of five minutes; therefore, a time period request of 12:40-13:40 actually displays data between 12:35-13:35. By default, the BIG-IP system displays one hour of data.*

You can continue to adjust the Custom Page so that it displays the information you want in the order you want it.

Scheduling Reports

Overview: Scheduling reports

You can schedule specific Analytics reports to be sent to one of more email addresses periodically. The reports that are available depend on the modules installed on your system, and how the system is configured. In the schedule, you specify the information to include in the report.

For example, if you are using Application Security Manager™ (ASM) to develop security policies, you can have the system send reports concerning attacks that were discovered, policy violations that occurred, and many other security measures. If you are a network administrator, you could schedule reports about DNS packets. Resource administrators can send reports so they can track CPU, disk, and memory utilization, and other system statistics. Many other reports are available that you can schedule to be sent regularly.

Scheduling reports to be sent

Before you can schedule reports to be sent, you need to configure SMTP on the system, and have the email addresses of the people to whom you want to send the reports.

You can set up schedules to send reports by email periodically. You select the information to include in the report.

1. On the main tab, click **Local Traffic** > **Profiles** > **Analytics** > **Scheduled Reports**.
   The Scheduled Reports screen opens.

   Note: *If SMTP is not configured, you receive a message with a link. Click the link to set up SMTP before proceeding.*

   ---

2. On the far right, click **Create**.
   The New Reporting Schedule screen opens.
3. In the **Name** field, type a name for the report schedule.
4. In the **Send To (E-Mails)** setting, type an email address where you want to send the report, and click **Add**.

   Add as many email addresses as you need to.
5. From the **SMTP Configuration** list, select the configuration that you want to use.

   If no configurations are available, click **Create** to add one.
6. From the **Reporting Module** list, select the type of report you want to send.

   The types of reports listed depend on which modules you have provisioned on your system. For example, if you have ASM and AFM provisioned, the list includes application security, DoS, and network firewall reports as well as reports showing general system statistics.
7. In the **Chart** setting, specify what you want to include in the report. Criteria and measures that you can specify vary for the different types of reports.
   a) In the **Filter** setting, from the lists, select the time period and number of results to show.
   b) In the **Chart Path**, select the top reporting criteria, then select the measures to include in the report.

      The criteria and measures differ depending on which **Reporting Module** you select.
   c) From the **Available measures**, select the ones to include in the report and move them to **Selected measures**.

d) To drill down and include more specific report criteria, click +, then from the **Use top result** list, select another option.
e) To include an average of all the statistics and the specific ones, select the **Include Overall** check box below the measures.

8. For **Mail Frequency**, select how often, the date to start, and the time to send the reports.
9. Click **Finished**.

The report schedule is added to the list. The specified report is sent by email to the addresses as scheduled. Or, select the schedule and click **Send Now** to test sending it right away. The report is attached to the email as a PDF. You can check the status in the list to see if the report was sent successfully.

Notes on Scheduled Reports

You can access Scheduled Reports from three places on the BIG-IP® system. The screen is the same, but the types of reports that you can schedule in each place varies.

- **Local Traffic** > **Profiles** > **Analytics** > **Scheduled Reports**: Lets you view and schedule reports for all provisioned modules, such as Application Security Manager ™and Advanced Firewall Manager, as well as for TMSTAT-related statistics, and health-related and network statistics including those for disk utilization, TCP, UDP, memory, CPU, DNS, and so on. (Requires user role of Administrator.)
- **Statistics** > **Analytics** > **Scheduled Reports**: Lets you view and schedule reports concerning overall system health-related and network statistics, including those for disk utilization, TCP, UDP, memory, CPU, DNS, and so on. (User roles can be Administrator, Resource Administrator, Application Security Administrator, or Application Security Editor.)
- **Security** > **Reporting** > **Scheduled Reports**: Lets you schedule reports that focus on provisioned security modules, including Application Security Manager and Advanced Firewall Manager. (User roles can be Administrator, Resource Administrator, Application Security Administrator, or Application Security Editor.)

If you have Administrator user privileges, you can schedule all of the reports. If you are a security or network administrator, you would schedule the reports through the Security or Statistics areas.

Scheduling predefined ASM reports to be sent

Before you can schedule reports to be sent, you need to configure SMTP on the system, and have the email addresses of the people to which you want to send the reports.

Application Security Manager™ (ASM) provides several predefined reports that list the top security issues discovered on the system. You can set up schedules to send one of the predefined ASM reports by email periodically.

1. On the main tab, click **Security** > **Reporting** > **Scheduled Reports**.
   The Scheduled Reports screen opens.

   Note: *If SMTP is not configured, you receive a message with a link. Click the link to set up SMTP before proceeding.*

2. On the far right, click **Create**.
   The New Reporting Schedule screen opens.
3. In the **Name** field, type a name for the report schedule.
4. In the **Send To (E-Mails)** setting, type an email address where you want to send the report, and click **Add**.

   Add as many email addresses as you need to.
5. From the **SMTP Configuration** list, select the configuration that you want to use.

   If no configurations are available, click **Create** to add one.

6. From the **Reporting Module** list, select **Application Security**.
7. In the **Chart** setting, specify the predefined report to send.
   a) Click **Predefined report**.
   b) From the list of predefined reports, select the one to send.
   c) To include an average of all the statistics and the specific ones, select the **Include Overall** check box below the list.
8. For **Mail Frequency**, select how often, the date to start, and the time to send the reports.
9. Click **Finished**.

The report schedule is added to the list. The predefined report is sent by email to the addresses as scheduled. Or, select the schedule and click **Send Now** to test sending it right away. The report is attached to the email as a PDF. You can check the status in the list to see if the report was sent successfully.

Investigating Server Latency Issues

Overview: Investigating server latency issues

This implementation describes how to investigate server latency on the BIG-IP® system. You can investigate server latency issues on the Analytics charts when Application Visibility and Reporting (AVR) is provisioned.

Investigating the server latency of applications

Before you can investigate server latency, you need to have created an HTTP Analytics profile that is logging statistics internally on the BIG-IP® system. The HTTP Analytics profile must be associated with one or more virtual servers, or with an iApps® application service.

You can review statistics concerning server latency on the HTTP Overview chart. *Server latency* is how long it takes (in milliseconds) from the time a request reaches the BIG-IP system, for it to proceed to the web application server, and return a response to the BIG-IP system.

1. On the Main tab, click **Statistics** > **Analytics** > **HTTP**.
   The Overview screen opens and displays current HTTP statistics averaged over the last hour. On the screen, you can see time controls on the top, charts on the left, and a list of dimensions on the right.
2. Scroll down to the Avg Server Latency chart.
   The chart shows the server latency for all applications and virtual servers associated with all Analytics profiles.
3. To view server latency for a specific application, from the dimensions on the right, expand **Applications** and select only that application.
   The chart shows latency only for the selected application.
4. To see more detailed latency statistics for any expanded dimensions, click the handle at the top of the dimensions column,
   Tables containing detailed statistics for the items in the dimensions are displayed.
5. In the table, hover over the headings to see the full names of the columns, and view the data.
   - **Avg Server Latency (ms)** shows the average server latency in milliseconds.
   - **Min Server Latency (ms)** shows the minimum server latency in milliseconds.
   - **Max Server Latency (ms)** shows the maximum server latency in milliseconds.
6. To view the graphic charts and dimensions again, click the handle on the top left of the table.
7. To view server latency for a specific virtual server, from the dimensions on the right, expand **Virtual Servers** and select only that virtual server.
8. You can clear all filter selections or those for a dimension.
   - To clear all selections, click the gear icon at the top of the column and select **Clear All**.
   - To clear selections for a dimension, click the options icon (three horizontal lines to the left of the title), and select **Clear Selection**.
9. If further investigation is needed, select other dimensions to show latency for other entities, for example, specific pool members, URLs, countries, or client IP addresses.

Tip: *If you are concerned about server latency, you can configure the HTTP Analytics profile so that it sends an alert when the average server latency exceeds a number of milliseconds for some period of time. See Getting an alert when server latency is high.*

Getting an alert when server latency is high

Before you can configure the system to send alerts concerning server latency, you need to have created an HTTP Analytics profile to collect application statistics locally (**Statistics Logging Type** must have **Internal** selected). To set up email alerts, the default **analytics** profile must specify an SMTP configuration.

You can configure the BIG-IP® system to send an alert when server latency is high.

1. On the Main tab, click **Local Traffic** > **Profiles** > **Analytics** > **HTTP Analytics**.

   Tip: *To have the **Analytics** listed, you need to provision Application Visibility and Reporting (AVR) first.*

   The **Profiles: Analytics** screen opens.
2. Click the name of a previously created Analytics profile, or create a new one.
3. Select the **Custom** check box.
4. For the **Statistics Logging Type** setting, verify that **Internal** is selected. If it is not, select it.

   Selecting **Internal** causes the system to store statistics locally, and you can view the charts on the system by starting at the Main tab, and clicking **Statistics** > **Analytics**.
5. To send email alerts, specify an **SMTP Configuration** (this can only be done on the default **analytics** profile).

   If you created a new profile, configure SMTP later.
6. For the **Notification Type** setting, select how you want the system to send alerts and notifications.

Option	Description
Syslog	Select **Syslog** if you want the system to send notification and alert messages to the local log system. You can view the messages on the **System** > **Logs** > **Local Traffic** screen.
SNMP	Select **SNMP** if you want the system to send notification and alert messages as SNMP traps. You can create the trap by clicking **Configuration can be found here** (**System** > **SNMP** > **Traps** > **Destination**). Enabling SNMP automatically sets up Syslog notifications, too.
E-mail	Select **E-mail** if you want the system to send notification and alert messages to email addresses. Type each email address in the **Notification E-Mails** field, and click **Add** to create the list. This option requires that the default analytics profile includes an SMTP configuration.

   When you select a notification type, the screen displays the Alerts and Notifications Configuration area, where you can indicate the criteria for alerts and notifications.
7. In the Alerts and Notifications Configuration area, for the **Add New Rule** setting, define the rule that determines when the system sends an alert about server latency.
   a) For **Alert when**, select **Average Server Latency**.
   b) Select **above**, and then type the number of milliseconds (the threshold) that is too high for your application. For example, type `100` if you want to receive an alert when latency is above 100 for 300 seconds.

      It is a good idea for you to get familiar with the typical average server latency of your application so you can recognize high server latency.
   c) Select **Application** as the granularity level to which the threshold applies.
   d) Click **Add**.
      The rule is added to the list of Active Rules.
8. Click **Update**.

9. If you need to configure SMTP (if sending alerts by email), click the default **analytics** profile on the Profiles: Analytics screen.
   a) For **SMTP Configuration**, select an existing configuration.
   b) If no SMTP configurations are listed, click the **here** link to create one. When you are done, you need to select the configuration you created in the default **analytics** profile.

The system sends an alert when the average server latency of an application exceeds 100 ms for 300 seconds. Another alert is sent when server latency changes back to under 100 ms for 300 seconds.

Viewing Application Page Load Times

Overview: Viewing application page load times

You can display the amount of time it takes for application web pages to load on client-side browsers. This information is useful if end users report that an application is slow, and you want to determine the cause of the problem. You can view page load times on the Analytics charts only if the HTTP Analytics profile for the web application is configured to save statistics concerning page load time.

The system can collect page load times only for clients using browsers that meet the following requirements:

- Support Navigation Timing by W3C
- Accept cookies from visited application sites
- Enable JavaScript® for the visited application sites

Viewing application page load times

Before you can view application page load times, you need to create an HTTP Analytics profile that is logging statistics internally on the BIG-IP® system. In the profile, the statistics-gathering configuration must have **Page Load Time** selected as one of the collected metrics. The Analytics profile also needs to be associated with one or more virtual servers, or an iApps® application service.

You can view page load times on the HTTP Overview chart. *Page load time* is how long (in milliseconds) it takes from the time an end user makes a request for a web page, until the web page from the application server finishes loading on the client-side browser.

Note: *End user response times and latencies can vary significantly based on geography and connection types.*

---

1. On the Main tab, click **Statistics** > **Analytics** > **HTTP**.
   The Overview screen opens and displays current HTTP statistics averaged over the last hour. On the screen, you can see time controls on the top, charts on the left, and a list of dimensions on the right.
2. Scroll down to the Avg Page Load Time chart.
   The chart shows the average page load time for all applications and virtual servers associated with all Analytics profiles.
3. To view page load time for a specific application, from the dimensions on the right, expand **Applications** and select only that application.
   The chart shows page load times only for the selected application.
4. To see more detailed page load time statistics for any expanded dimensions, click the handle at the top of the dimensions column,
   Tables containing detailed statistics for the items in the dimensions are displayed.
5. In the table, hover over the headings to see the full names of the columns, and view the data.
   - **Avg Pa** shows the average page load time in milliseconds.
   - **Max Pa** shows the maximum page load time in milliseconds.
6. To view page load times for a specific virtual server, from the dimensions on the right, expand **Virtual Servers** and select only that virtual server.
7. You can clear all filter selections or those for a dimension.

- To clear all selections, click the gear icon at the top of the column and select **Clear All**.
- To clear selections for a dimension, click the options icon (three horizontal lines to the left of the title), and select **Clear Selection**.

8. If further investigation is needed, select other dimensions to show page load times for other entities, for example, specific pool members, URLs, countries, or client IP addresses.

Tip: *If you are concerned about maintaining a high level of user experience and productivity, you can configure the Analytics profile so that it sends an alert when the average page load time exceeds a number of milliseconds for some period of time.*

Troubleshooting Applications by Capturing Traffic

Overview: Troubleshooting applications by capturing traffic

This implementation describes how to set up the BIG-IP® system to collect application traffic so that you can troubleshoot problems that have become apparent by monitoring application statistics. For example, by examining captured requests and responses, you can investigate issues with latency, throughput, or reduced transactions per second to understand what is affecting application performance.

When Application Visibility and Reporting (AVR) is provisioned, you can create an Analytics profile that includes traffic capturing instructions. The system can collect application traffic locally, remotely, or both. If the system is already monitoring applications, you can also update an existing Analytics profile to make it so that it captures traffic.

If logging locally, the system logs the first 1000 transactions and displays charts based on the analysis of those transactions. For VIPRION® systems, the local logging consists of the first 1000 transactions multiplied by however many blades are installed. If logging remotely, the system logs information on that system; log size is limited only by any constraints of the remote logging system. To see updated application statistics, you can clear the existing data to display the current statistics.

Task Summary

Capturing traffic for troubleshooting
Reviewing captured traffic

About prerequisites for capturing application traffic

After you finish a basic networking configuration of the BIG-IP® system, you must complete these prerequisites for setting up application statistics collection:

- Provision Application Visibility and Reporting (AVR): **System** > **Resource Provisioning**.
- Create an iApps® application service (go to **iApp** > **Application Services**), or configure at least one virtual server with a pool pointing to one or more application servers.

You can set up the system for capturing application traffic either locally or remotely (or both).

Tip: *Before setting up, clear the captured transaction log. On the Captured Transactions screen, click* ***Clear All*** *to clear all previously captured data records.*

Capturing traffic for troubleshooting

You typically use traffic capturing if you notice an application issue, such as trouble with throughput or latency, discovered when examining application statistics, and want to troubleshoot the system by examining actual transactions.

You can configure the BIG-IP® system to capture application traffic and store the information locally or remotely (on Syslog servers or SIEM devices, such as Splunk). To do this, you create an Analytics profile designed for capturing traffic. The profile instructs the BIG-IP system to collect a portion of application traffic using the Application Visibility and Reporting (AVR) module.

1. On the Main tab, click **Local Traffic** > **Profiles** > **Analytics** > **HTTP Analytics**.

Tip: *If **Analytics** is not listed, this indicates that Application Visibility and Reporting (AVR) is not provisioned, or you do not have rights to create profiles.*

The HTTP Analytics screen opens.

2. In the Profile Name column, click **analytics** (the name of the default profile).
3. In the General Configuration area, clear the **Transaction Sampling** check box.
   The system analyzes all traffic to the associated virtual servers.
4. Above the menu bar, click the **Profiles: Analytics** link to return to the Analytics list screen.
5. Click **Create**.
   The New HTTP Analytics profile screen opens.
6. In the **Profile Name** field, type a unique name for the Analytics profile.
7. Select the **Custom** check box.
8. For **Traffic Capturing Logging Type**, specify where to store captured traffic.
   - To store traffic locally, click **Internal**. You can view details on the Captured Transactions screen. This option is selected by default.
   - To store traffic on a remote logging server, click **External** and provide the requested information.
9. In the Associated Virtual Servers area, specify the virtual servers for which to capture application statistics:
   a) For the **Virtual Servers** setting, click **Add**.
   b) From the Select Virtual Server popup that displays, select the virtual servers to include and then click **Done**.

Note: *Only virtual servers previously configured with an HTTP profile display in the list (because the data being collected applies to HTTP traffic). Also, you can assign only one HTTP Analytics profile to a virtual server; therefore, the list displays only virtual servers that have not been assigned an Analytics profile.*

Special considerations apply if using Analytics on a BIG-IP system with both Application Security Manager™ and Access Policy Manager®, where security settings (in Portal Access webtop or an iRule) redirect traffic from one virtual server to another. In this case, you need to attach the HTTP Analytics profile to the second virtual server to ensure that the charts show accurate statistics.

10. If you want to make changes to any of the selections, above the Statistics Gathering Configuration area, select the **Custom** check box.
11. In the Statistics Gathering Configuration area, for **Collected Metrics**, select additional statistics you want the system to collect from the requests:

Option	Description
Max TPS and Throughput	Collects statistics showing the maximum number of transactions occurring per second and the amount of traffic moving through the system (maximum request and response throughput is collected and recorded separately).
Page Load Time	Tracks how long it takes an application user to get a complete response from the application, including network latency and completed page processing. ***Note:*** *End-user response times and latencies can vary significantly based on geography and connection types.*
User Sessions	Stores the number of unique user sessions. For **Timeout**, select the number of minutes of user inactivity to allow before the system considers the session to be over.

Option	Description
	For **Cookie Secure Attribute**, specify whether to secure session cookies. Options are **Always**, the secure attribute is always added to the session cookie; **Never**, the secure attribute is never added to the session cookie; or **Only SSL**, the secure attribute is added to the session cookie only when the virtual server has a client SSL profile (the default value).

By default, the system collects many metrics, including TPS, throughput, server latency, response time, network latency, and so on. You can select the ones here in addition to the ones already collected once the Analytics profile is attached to one or more virtual servers.

12. In the Statistics Gathering Configuration area, for **Collected Entities**, select additional entities to collect statistics for each request.

Option	Description
URLs	Collects the requested URLs.
Countries	Saves the name of the country where the request came from, and is based on the client IP address criteria.
Client IP Addresses	Saves the IP address where the request originated. The address saved also depends on whether the request has an XFF (X-forwarded-for) header and whether the HTTP profile accepts XFF headers.
Client Subnets	Saves statistics for predefined client subnets. Client subnets can be added in the Subnets area of the default HTTP Analytics profile.
Response Codes	Saves HTTP response codes that the server returned to requesters.
User Agents	Saves information about browsers making the request.
Methods	Saves HTTP methods in requests.

By default, the system collects many entity statistics, including virtual servers, pool members, browser names, operating system, and so on. You can select the ones here in addition to the ones already collected once the Analytics profile is attached to one or more virtual servers.

13. In the Capture Filter area, from the **Capture Requests** and **Capture Responses** lists, select the options that indicate the part of the traffic to capture.

Option	Description
None	Specifies that the system does not capture request (or response) data.
Headers	Specifies that the system captures request (or response) header data only.
Body	Specifies that the system captures the body of requests (or responses) only.
All	Specifies that the system captures all request (or response) data.

14. Depending on the application, customize the remaining filter settings to capture the portion of traffic to that you need for troubleshooting.

Tip: *By focusing in on the data and limiting the type of information that is captured, you can troubleshoot particular areas of an application more quickly. For example, capture only requests or responses, specific status codes or methods, or headers containing a specific string.*

---

15. Click **Finished**.

The BIG-IP system captures the application traffic described by the Analytics profile for 1000 transactions locally (or until system limits are reached). If logging remotely, the system logs information on that system; log size is limited only by constraints of the remote logging system.

Note: *System performance is affected when traffic is being captured.*

Reviewing captured traffic

Before you can review captured traffic details on the BIG-IP® system, you need to create an HTTP Analytics profile that is capturing application traffic locally. The settings you enable in the Capture Filter area of the profile determine what information the system captures. You need to associate the Analytics profile with one or more virtual servers, or with an iApps® application service.

The system starts capturing application traffic as soon as you enable it on the HTTP Analytics profile. You can review the captured transactions locally on the BIG-IP system. The system logs the first 1000 transactions. On a VIPRION® system, the system logs the first 1000 transactions multiplied by however many blades are installed.

1. On the Main tab, click **System** > **Logs** > **Captured Transactions**.
   The Captured Transactions screen opens and lists all of the captured transactions.
2. Optionally, use the time period and filter settings to limit which transactions are listed.
3. In the Captured Traffic area, click any transaction that you want to examine.
   Details of the request display on the screen.
4. Review the general details of the request.

   Tip: *The general details, such as the response code or the size of the request and response, help with troubleshooting.*

5. For more information, click **Request** or **Response** to view the contents of the actual transaction.

   Review the data for anything unexpected, and other details that can help troubleshoot the application.
6. On the Captured Transactions screen, click **Clear All** to clear all previously captured data records (including those not displayed on the screen) and start collecting transactions again.
   The system captures up to 1000 transactions locally and displays them on the screen. Captured transactions are visible a few seconds after they occur.

Using Local Traffic Policies with Analytics

Overview: Using local traffic policies with Analytics

When you attach an Analytics (AVR) profile to a virtual server, the BIG-IP® system can gather, log, notify, and display statistical information about the traffic. You can associate a local traffic policy with a virtual server to further define which transactions to include or exclude in the statistics. Rules in the local traffic policy can enable or disable AVR for whatever type of traffic you want to define. You might want to do this to save system resources by not deploying Analytics on parts of the traffic that you are not interested in monitoring.

This implementation shows how to create an HTTP Analytics profile to store statistics locally. It then describes how to create a local traffic policy and add rules to the policy so that the Analytics module saves statistics for all traffic except that which has a URI containing the word `index`. (In this case, you are not interested in monitoring traffic directed towards index pages.)

Other options are available for configuring local traffic policies with Analytics. By following through the steps in this example, you can see the other options that are available on the screens, and can adjust the example for your needs.

Task Summary

Collecting application statistics locally

You need to provision the Application Visibility and Reporting (AVR) module before you can collect application statistics locally.

You can configure the BIG-IP® system to collect specific application statistics locally.

1. On the Main tab, click **Local Traffic** > **Profiles** > **Analytics** > **HTTP Analytics**.

   Tip: *If **Analytics** is not listed, this indicates that Application Visibility and Reporting (AVR) is not provisioned, or you do not have rights to create profiles.*

   The HTTP Analytics screen opens.
2. Click **Create**.
   The New HTTP Analytics profile screen opens.
3. In the **Profile Name** field, type a unique name for the Analytics profile.
4. From the **Parent Profile** list, select the profile from which you want to inherit settings.

   The default profile is often used as the parent profile.

   The new profile inherits the values from the parent profile. If the parent is changed, the inherited values in the new profile also change.
5. Select the **Custom** check box.
6. For the **Statistics Logging Type** setting, verify that **Internal** is selected. If it is not, select it.

   Selecting **Internal** causes the system to store statistics locally, and you can view the charts on the system by starting at the Main tab, and clicking **Statistics** > **Analytics**.

7. You can use the default values for the rest of the General Configuration settings.
8. In the Associated Virtual Servers area, specify the virtual servers for which to capture application statistics:
   a) For the **Virtual Servers** setting, click **Add**.
   b) From the Select Virtual Server popup that displays, select the virtual servers to include and then click **Done**.

   Note: *Only virtual servers previously configured with an HTTP profile display in the list (because the data being collected applies to HTTP traffic). Also, you can assign only one HTTP Analytics profile to a virtual server; therefore, the list displays only virtual servers that have not been assigned an Analytics profile.*

   Special considerations apply if using Analytics on a BIG-IP system with both Application Security Manager™ and Access Policy Manager®, where security settings (in Portal Access webtop or an iRule) redirect traffic from one virtual server to another. In this case, you need to attach the HTTP Analytics profile to the second virtual server to ensure that the charts show accurate statistics.
9. In the Statistics Gathering Configuration area, select the **Custom** check box.
10. In the Statistics Gathering Configuration area, for **Collected Metrics**, select additional statistics you want the system to collect from the requests:

Option	Description
Max TPS and Throughput	Collects statistics showing the maximum number of transactions occurring per second and the amount of traffic moving through the system (maximum request and response throughput is collected and recorded separately).
Page Load Time	Tracks how long it takes an application user to get a complete response from the application, including network latency and completed page processing. ***Note:*** *End-user response times and latencies can vary significantly based on geography and connection types.*
User Sessions	Stores the number of unique user sessions. For **Timeout**, select the number of minutes of user inactivity to allow before the system considers the session to be over. For **Cookie Secure Attribute**, specify whether to secure session cookies. Options are **Always**, the secure attribute is always added to the session cookie; **Never**, the secure attribute is never added to the session cookie; or **Only SSL**, the secure attribute is added to the session cookie only when the virtual server has a client SSL profile (the default value).

   By default, the system collects many metrics, including TPS, throughput, server latency, response time, network latency, and so on. You can select the ones here in addition to the ones already collected once the Analytics profile is attached to one or more virtual servers.
11. In the Statistics Gathering Configuration area, for **Collected Entities**, select additional entities to collect statistics for each request.

Option	Description
URLs	Collects the requested URLs.
Countries	Saves the name of the country where the request came from, and is based on the client IP address criteria.
Client IP Addresses	Saves the IP address where the request originated. The address saved also depends on whether the request has an XFF (X-forwarded-for) header and whether the HTTP profile accepts XFF headers.

Option	Description
Client Subnets	Saves statistics for predefined client subnets. Client subnets can be added in the Subnets area of the default HTTP Analytics profile.
Response Codes	Saves HTTP response codes that the server returned to requesters.
User Agents	Saves information about browsers making the request.
Methods	Saves HTTP methods in requests.

By default, the system collects many entity statistics, including virtual servers, pool members, browser names, operating system, and so on. You can select the ones here in addition to the ones already collected once the Analytics profile is attached to one or more virtual servers.

12. Click **Finished**.

The BIG-IP system collects the statistics specified in the Analytics profile. You can view the statistics by clicking **Statistics** > **Analytics**.

Creating a local traffic policy for Analytics

Before you can create a local traffic policy for Analytics, you need to provision the Application Visibility and Reporting (AVR) module.

You can create a local traffic policy to define which traffic should be included (or excluded) from Analytics statistics collection. This example creates one rule that looks at all traffic and excludes traffic that has the word "index" in the URI.

1. On the Main tab, click **Local Traffic** > **Policies** > **Policy List**.
   The Policy List Page screen opens.
2. Click **Create**.
   The New Policy screen opens.
3. In the **Policy Name** field, type a unique name for the policy.
4. For the **Strategy**setting, select **first** to apply the actions in the first rule that matches.
5. If you see a **Type** setting, leave it set to **Traffic Policy**.
6. Click **Create Policy**.
   The Draft Policy screen opens.
7. In the Rules area, click **Create** to create a rule that defines when traffic is handled by the security policy.
8. In the **Name** field, type the word `index`.
9. In the Match all of the following conditions area, click + and specify these conditions:
   a) For the first condition, select **HTTP URI**.
   b) For the second condition, select **path**.
   c) For the third condition, select **contains**.
   d) For the fourth condition, by the field below **any of**, type `index` and click **Add**.

   This rule looks for requests with a URI that contains the word "index".
10. In the Do the following when the traffic is matched area, click + and specify the actions:
    a) For the first action, select **Disable**.
       For the second action, select **avr**.
11. Click **Save** to add the rule to the local traffic policy.
    The policy properties screen opens.
12. Create a default rule that tells the system to store statistics for all other traffic.
    a) In the Rules area, click **Create**.

b) In the **Name** field, type the word `default`.
c) Leave **Match all of the following conditions** set to **All traffic**.
d) In the Do the following when the traffic is matched area, click +.
e) For the actions, select **Enable**, then **avr**.
f) Click **Save** to add the rule to the local traffic policy.

13. To save the updated policy, click **Save Draft**.
The Policy List Page opens.
14. Select the check box next to the draft policy you edited, and click **Publish**.

You have created and published a local traffic policy that controls Analytics. It looks at all traffic and disables statistics gathering for any request that includes the word `index` in the URI. For all other traffic, statistics are collected.

Associating a published local traffic policy with a virtual server

After you publish a local traffic policy, you associate that published policy with the virtual server created to handle application traffic.

1. On the Main tab, click **Local Traffic** > **Virtual Servers**.
The Virtual Server List screen opens.
2. Click the name of the virtual server you want to modify.
3. On the menu bar, click **Resources**.
4. In the Policies area, click the **Manage** button.
5. For the **Policies** setting, select the local traffic policy you created from the **Available** list and move it to the **Enabled** list.
6. Click **Finished**.

The published policy is associated with the virtual server.

Implementation results

When you have completed the steps in this implementation, you have configured the BIG-IP® system to store statistics locally. A local traffic policy instructs the Analytics module to save statistics for all traffic except that which has a URI containing the word `index`.

Viewing System-Level Statistics

Overview: Viewing system level statistics

You can display system level statistics over a period of time in graphical charts on the BIG-IP® system. Several charts are available, and they show the following information:

- Internet Protocol (IP) packets, errors, and fragments
- Virtual server traffic details, TCP traffic, and UDP traffic
- CPU usage
- CPU utilization per process
- Memory statistics for TMM, other processes, system RAM, and swap space
- Disk activity, sizes, and latency

You can view the historical statistics for different periods of time. On systems with multiple slots, you can view the statistics for each slot. You can also export the information in any of the reports to PDF or comma-separated value (CSV) format, and save the reports or email them.

Viewing CPU, disk, and memory statistics

Before you can view the system analytics charts described here, you need to provision the Application Visibility and Reporting (AVR) module.

You can view CPU, disk, and memory statistics for the BIG-IP® system to help with system troubleshooting.

1. To view CPU statistics, on the Main tab, click **Statistics** > **Analytics>** > **CPU**.
   The CPU statistics chart opens showing CPU usage over time.
2. From the **View By** list, select the item for which to display statistics.

   Tip: *You can also click* ***Expand Advanced Filters*** *to filter the information that displays.*
3. From the **Time Period** list, select the length of time for which to display statistics.
4. To focus in on the specific details you want more information about, click the chart or an item in the details list.

   Tip: *This works on any of the Analytics charts.*
5. To view memory statistics, on the Main tab, click **Statistics** > **Analytics>** > **Memory**.
   The Memory TMM statistics chart opens showing the average total RAM used per slot over a period of time.
6. Click the other items on the menu bar to see additional memory use.
   - To see other usage, such as management use, click **Other**.
   - To see operating system usage, click **System**.
   - To see how much swap is being used, click **Swap**.
7. To view disk statistics, on the Main tab, click **Statistics** > **Analytics>** > **Disk**.
   The Disk Activity statistics chart opens showing the average total RAM used per slot over a period of time.
8. Click the other items on the menu bar to see additional disk use statistics.
   - To see read or write bytes over time, click **Disk Sizes**.
   - To see read latency, click **Disk Latency**.

9. If you want to export the information in any of the charts, click **Export** and specify your options for how and where to send the data.

   To send reports by email, the system requires an SMTP configuration.

The statistics provide an overview of CPU, disk, and memory use on the system. As a result, you become more familiar with the system and its resource utilization, and you can troubleshoot the system as needed.

Sample CPU statistics

This figure shows a sample CPU statistics report showing the percentage of CPU usage per CPU for the past week. This BIG-IP® system has 4 CPUs, all in use.

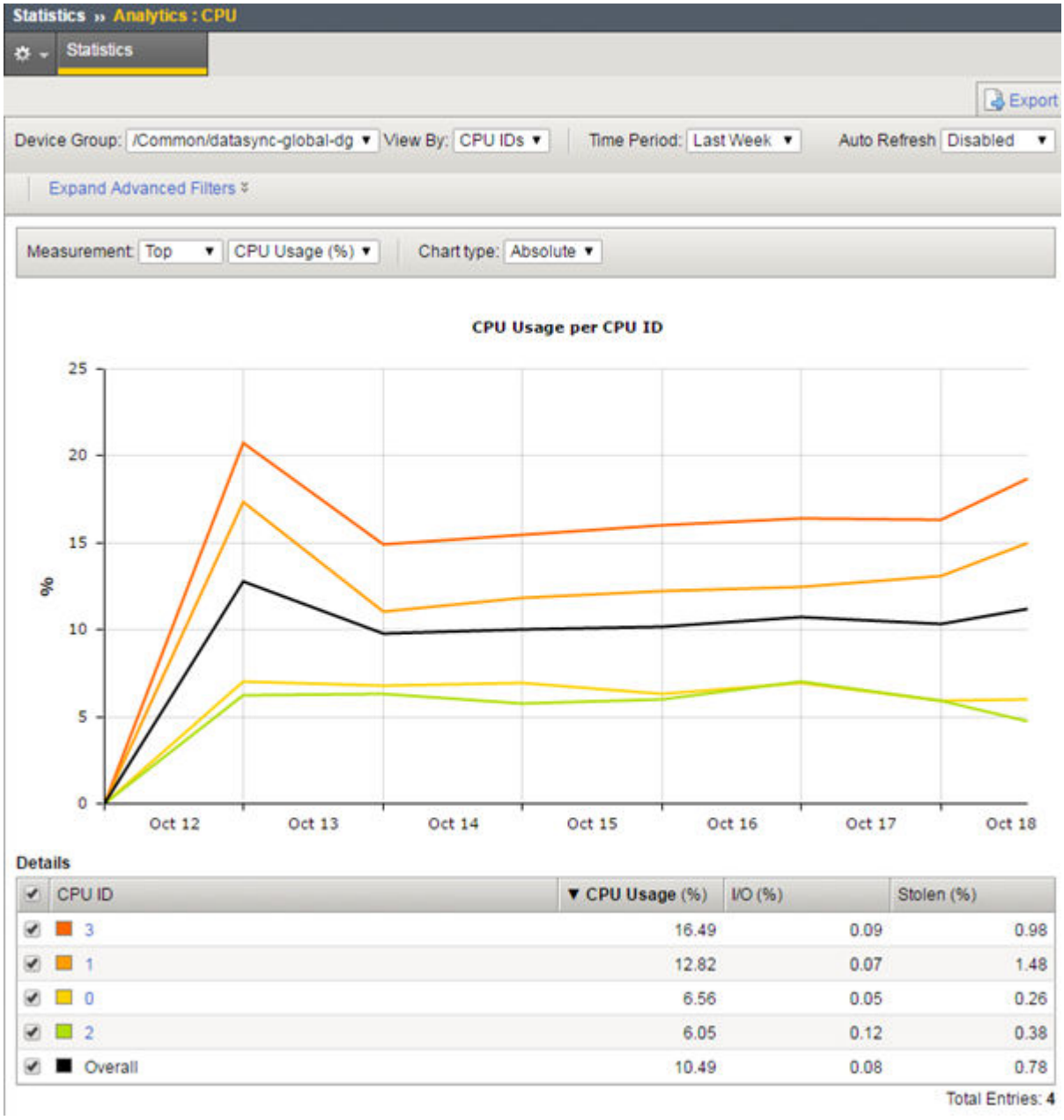


Figure 1: Sample CPU statistics

Sample system memory statistics

This sample chart shows system RAM memory in use for the past week. This system has two slots. In this figure, the average RAM went from 0 to 11.166 GB per slot.

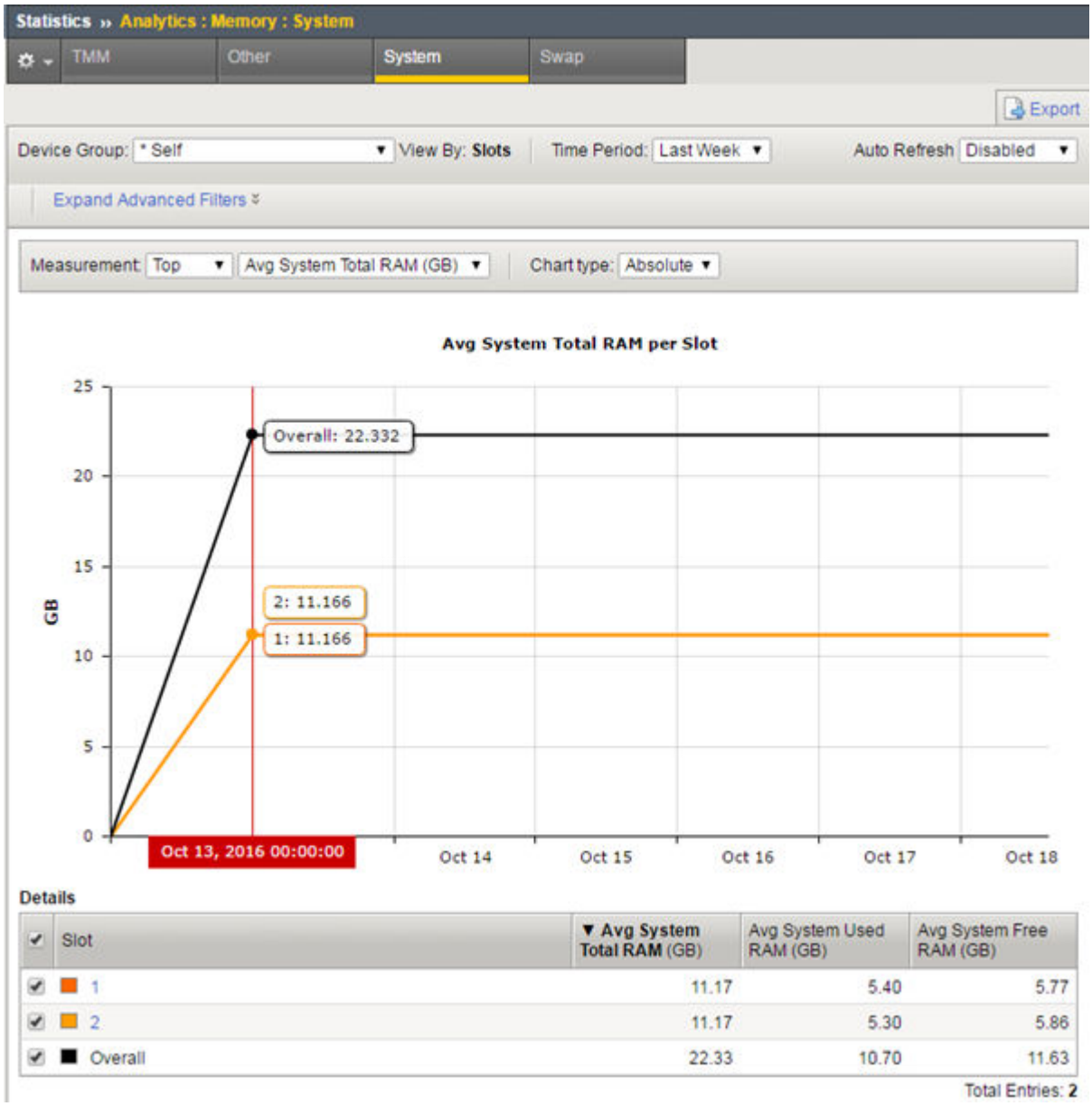


Figure 2: Sample system memory chart

You can see other memory statistics by selecting **TMM**, **Other**, or **Swap** on the menu bar.

Sample disk statistics

This sample chart shows disk activity for the past hour. It shows that the total I/O activity on the two slots was 39,700 I/O operations.

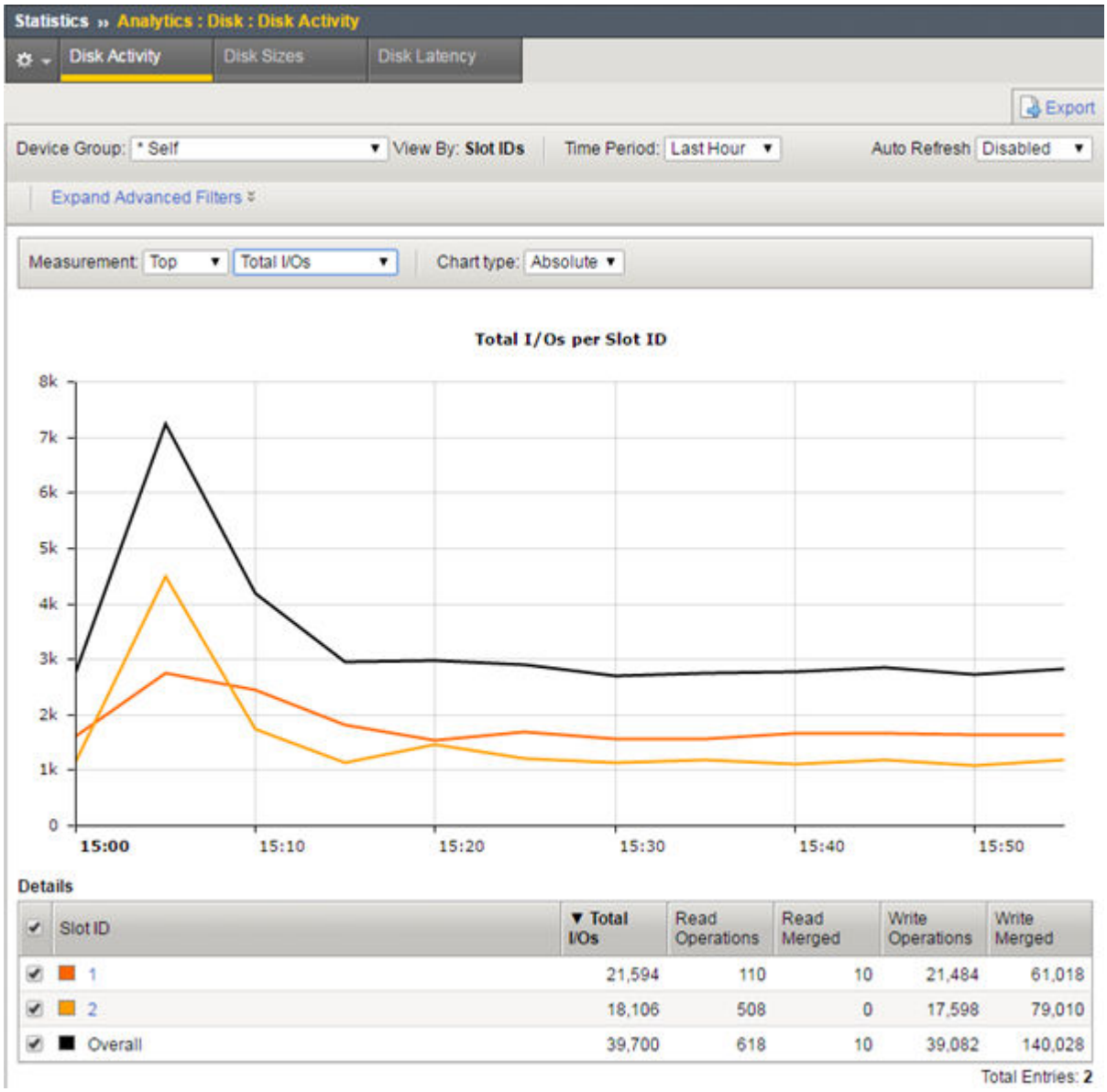


Figure 3: Sample Disk Activity chart

Viewing CPU usage per process

Before you can view the system analytics charts described here, you need to provision the Application Visibility and Reporting (AVR) module.

On the BIG-IP® system, you can view average CPU usage per process (or per blade on multi-blade systems) to help with system troubleshooting. The system displays CPU usage information for the top 10 processes as a percentage. On multi-blade systems, the chart shows statistics for each blade.

1. To view CPU usage per process, on the Main tab, click **Statistics** > **Analytics** > **Process CPU Utilization**.
   The Process CPU Utilization chart opens showing CPU usage per process on the system.
2. From the **View By** list, select the item for which to display statistics.
   You can view the CPU usage details by processes, blade numbers, or process IDs.

Tip: *You can also click* ***Expand Advanced Filters*** *to further filter the information that displays.*

---

3. From the Time Period list, select the length of time for which to display statistics.
4. To focus in on the specific details you want more information about, click the chart or an item in the details list.

   Tip: *This works on any of the Analytics charts.*

5. If you want to export the information in any of the charts, click **Export** and specify your options for how and where to send the data.

   To send reports by email, the system requires an SMTP configuration.

The charts show how much CPU processing power each process is using.

Sample CPU usage statistics

This sample CPU usage report shows the percentage of CPU usage per process for the past day. This BIG-IP® system is running Analytics (AVR), Local Traffic Manager™ (LTM), Application Security Manager™ (ASM), and Advanced Firewall Manager™ (AFM), so you can see the processes associated with those products.

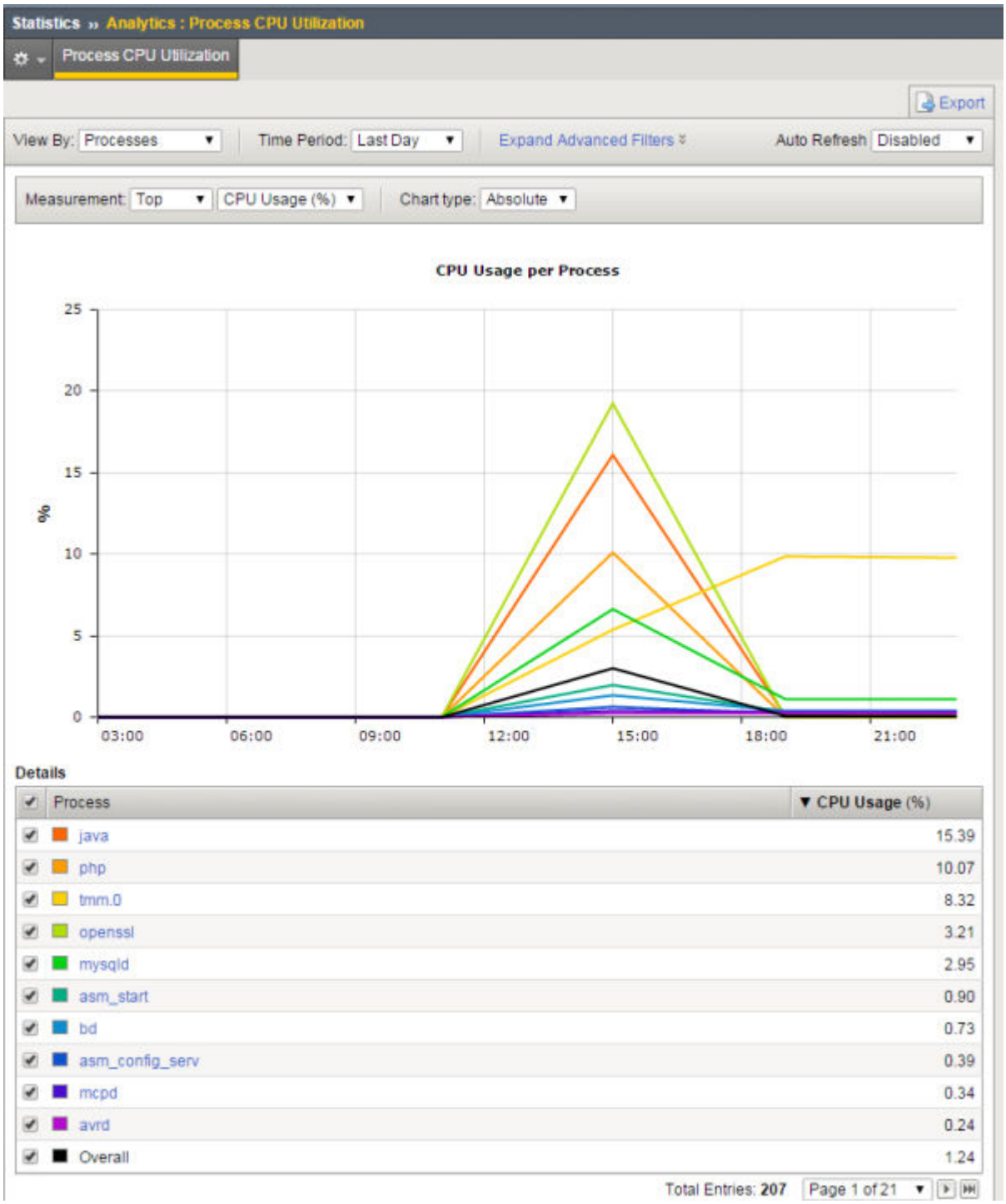


Figure 4: Sample CPU statistics

Note: *The statistics displayed are rounded up to two decimal digits.*

The top 10 processes are color-coded and listed in the chart and details table. For example, `avrd` is the daemon that collects data for AVR™, and `bd` is the main enforcement engine for ASM™. The process called `tmm.0` is the Traffic Management Microkernel (TMM), a core system process that manages traffic on the BIG-IP system.

Viewing network statistics

Before you can view network analytics charts, you need to provision the Application Visibility and Reporting (AVR) module.

You can view network statistics for the BIG-IP® system to help with system troubleshooting and understanding peak load times. Statistics are available at both the Internet Protocol (IP) and virtual server level.

1. To view CPU statistics, on the Main tab, click **Statistics** > **Analytics** > **IP**.
   The IP Packets chart opens showing packets transmitted for IPv4 and IPv6 over time.
2. From the Time Period list, select the length of time for which to display statistics.
3. To focus in on the specific details you want more information about, click the chart or an item in the details list.

   Tip: *This works on any of the Analytics charts.*
4. Click the other items on the menu bar to see information about IP errors and fragments.
5. To view virtual server statistics, on the Main tab, click **Statistics** > **Analytics** > **Virtual Servers**.
   The Virtual Servers Traffic Details chart opens showing the total client connections per virtual server over a period of time.
6. Click the other items on the menu bar to see packet use or information in bits.
7. To focus in on one virtual server, click it on the chart or in the details list.
8. To view TCP connections, on the Main tab, click **Statistics** > **Analytics** > **Virtual Servers** > **TCP**.
   The TCP connections chart opens showing the average connections per virtual server over a period of time.
9. Click the other items on the menu bar to see additional TCP statistics.
   - To see various TCP packets, click **Packets** and adjust the measurements for different views.
   - To see information about SYN Cookies, such as the total received, click **SynCookies**.
10. To view UDP connections, on the Main tab, click **Statistics** > **Analytics** > **Virtual Servers** > **UDP**.
    The UDP connections chart opens showing the average connections per virtual server over a period of time.
11. Click **Datagrams** on the menu bar to see additional UDP statistics such as the total datagrams received and the total number of datagrams that were malformed.
12. If you want to export the information in any of the charts, click **Export** and specify your options for how and where to send the data.

    To send reports by email, the system requires an SMTP configuration.

The statistics provide an overview of what is happening on the system network. You can drill down to see specific statistics for different protocols and specific virtual servers.

Sample IP Packets report

This sample IP Packets report shows the number of packets received in both IPv4 and IPv6 formats during the past day. Most of the traffic is in IPv4.

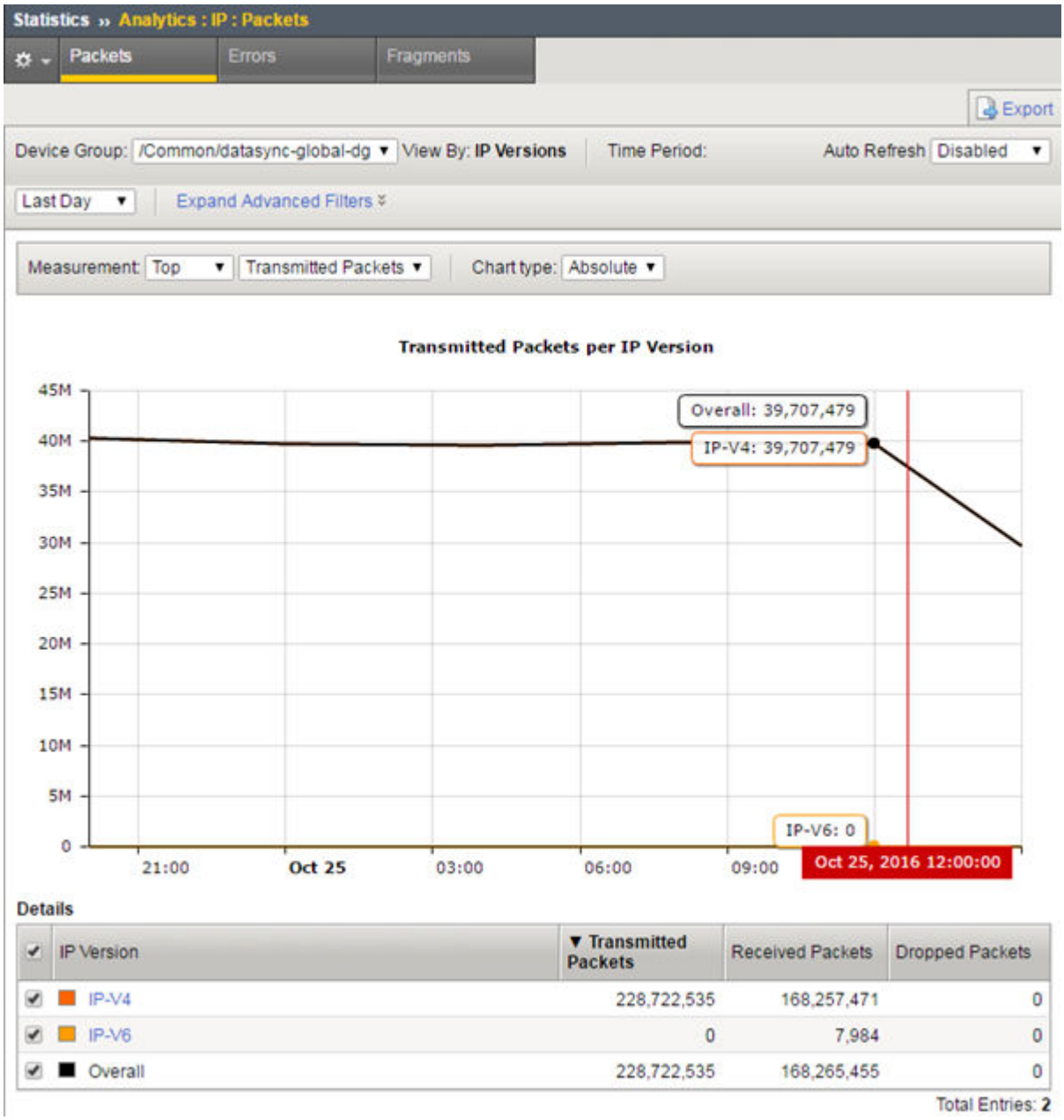
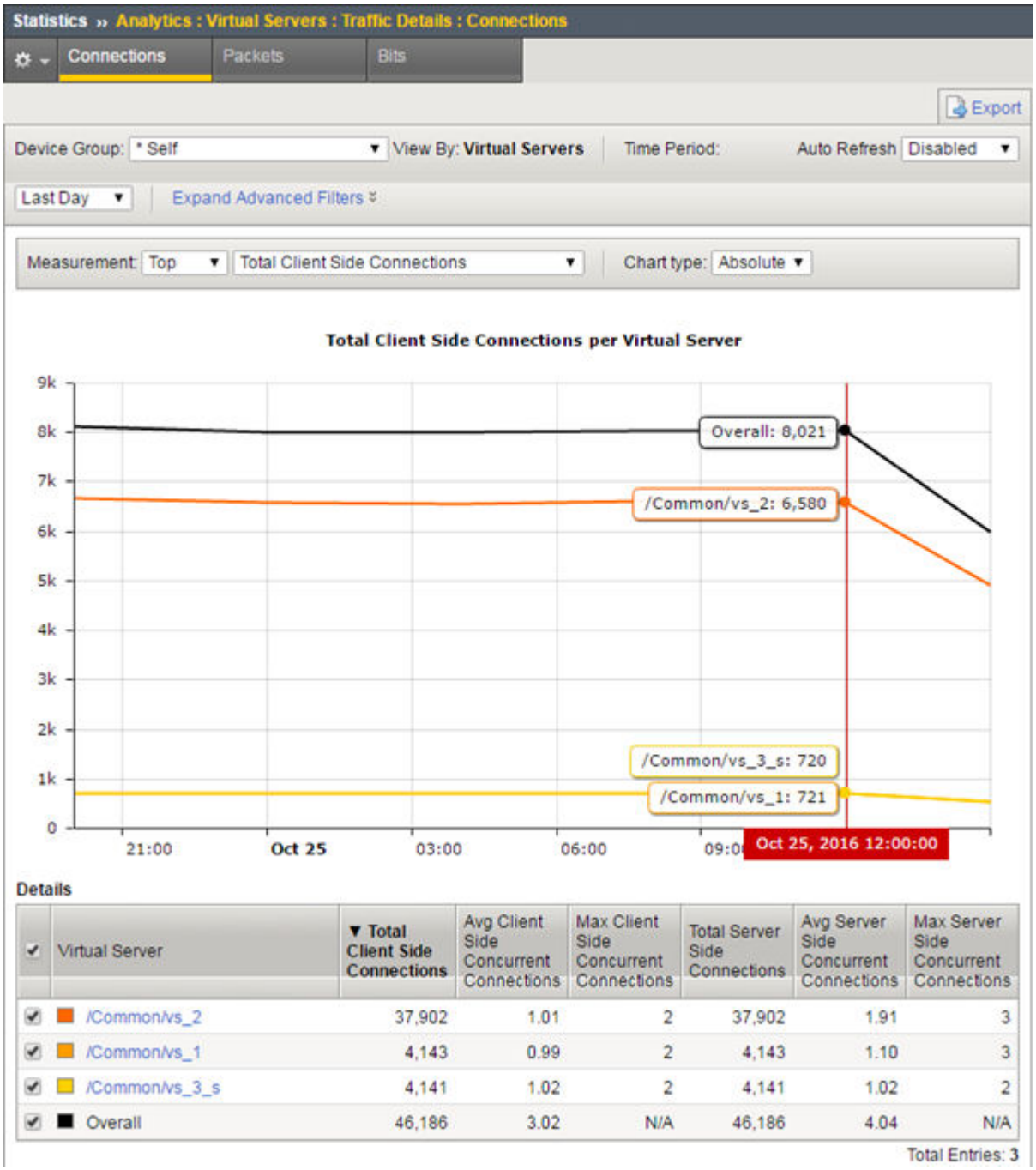


Figure 5: Sample IP Packets report

Sample Virtual Servers report

This sample Virtual Servers report shows the number of client connections per virtual server. All of the traffic is on three virtual servers. By placing the cursor at the highest point, the screen shows details of the number of overall connections, the connections per virtual server, and the time. This way you can monitor peak usage times.



Details

Virtual Server	▼ Total Client Side Connections	Avg Client Side Concurrent Connections	Max Client Side Concurrent Connections	Total Server Side Connections	Avg Server Side Concurrent Connections	Max Server Side Concurrent Connections
/Common/vs_2	37,902	1.01	2	37,902	1.91	3
/Common/vs_1	4,143	0.99	2	4,143	1.10	3
/Common/vs_3_s	4,141	1.02	2	4,141	1.02	2
Overall	46,186	3.02	N/A	46,186	4.04	N/A

Total Entries: 3

Figure 6: Sample Virtual Servers Traffic report

Collecting and Viewing TCP Statistics

Overview: Viewing TCP statistics

You can set up the BIG-IP® system to gather information about TCP flows to better understand what is happening on your networks. The system can collect TCP statistics locally, remotely, or both. You can view these statistics in graphical charts, and use the information for troubleshooting and improving network performance.

The statistic reports for both TCP and FastL4 show details about RTT (round trip time), goodput, connections, and packets. For TCP, you can also view statistics for delay analysis. You can save the reports or email them to others.

Task Summary

Creating a TCP Analytics profile
Viewing TCP statistics

Creating a TCP Analytics profile

Before you can create a TCP profile, you must have provisioned the Application Visibility and Reporting (AVR) module.

A TCP Analytics profile directs the system to store TCP statistics about specific entities for use in diagnosing network problems. The Application Visibility and Reporting (AVR) module includes a default TCP Analytics profile called `tcp-analytics`. You can edit the values in the default profile, or create a new one, as described here.

1. On the Main tab, click **Local Traffic** > **Profiles** > **Analytics** > **TCP Analytics**.

   Tip: *If **Analytics** is not listed, you need to provision Application Visibility and Reporting (AVR) first.*

   The **TCP Analytics** screen opens.
2. Click **Create**.
   The New TCP Analytics Profile screen opens, inheriting values from the system-supplied TCP Analytics profile.
3. For **Profile Name**, type a name for the profile.
4. From the **Parent Profile** list, select the profile from which you want to inherit settings.

   The default profile is often used as the parent profile.

   The new profile inherits the values from the parent profile. If the parent is changed, the inherited values in the new profile also change.
5. To make the fields editable, click **Custom** in the upper right corner.

   Tip: *If you don't need to change any of the values, just use the default profile instead.*
6. For the **Statistics Logging Type** setting, verify that **Internal** is selected. If it is not, select it.

   Selecting **Internal** causes the system to store statistics locally, and you can view the charts on the system by starting at the Main tab, and clicking **Statistics** > **Analytics**.
7. For **Statistics Collection**, leave the default, **Client side**, selected.

   This option specifies where the system gets the statistics from.

8. In the Associated Virtual Servers area, specify the virtual servers that use this TCP Analytics profile to capture TCP statistics:
   a) For the **Virtual Servers** setting, click **Add**.
   b) From the Select Virtual Server popup screen that displays, select the virtual servers to include, and then click **Done**.

   Note: *Only virtual servers previously configured to use TCP protocol or FastL4 (Type Performance Layer 4) display in the list (because the data being collected applies to TCP or FastL4 traffic). Also, you can assign only one TCP Analytics or HTTP Analytics profile to a virtual server; therefore, the list displays only virtual servers that have not been assigned either of these profiles.*

   The system attaches the profile to the virtual servers you added.
9. In the Statistics Gathering Configuration area, for **Collected Entities**, select the entities for which you want the system to collect information.

   Note: *The more entities you enable, the greater the impact on system performance.*

10. Click **Finished**.

The system creates the TCP Analytics profile. If the BIG-IP® system is exchanging traffic with clients, TCP statistics are collected for the virtual servers and collected entities specified in this profile.

Note: *To view RTT statistics for Layer 4 traffic managed using a FastL4 profile, you also need to enable* ***RTT from Client*** *and* ***RTT from Server*** *(as appropriate) in the FastL4 profile.*

If later you decide you want to store TCP analytics remotely, you can use the external Statistics Logging Type and specify a remote publisher to specify where to send the statistics.

Viewing TCP statistics

Before you can view TCP statistics, you must have created a TCP Analytics profile that is logging statistics internally on the BIG-IP® system. The TCP Analytics profile also needs to be associated with one or more virtual servers.

You can view TCP statistics in the Analytics charts.

1. On the Main tab, click **Statistics** > **Analytics** > **TCP**.
   The RTT statistics screen opens.
2. For **Time Period**, you can adjust the time frame for which to display the data.
3. To look at the statistics from a different point of view, for **View By**, select the category of data to display in the chart.

   You can also click an item in the Details list to drill down and display more specific statistics.

   The screen displays data in the categories for which you are saving statistics in the TCP Analytics profile.
4. Click any item on the menu bar to see different TCP Analytics charts.

Click This	To View These Statistics
RTT	Round trip times from the BIG-IP system to the remote host and back.
Goodput	Throughput at the application level used to review overall network performance. It shows total throughput aggregated for all connections on the configured entities.
Delay State	The aggregate time spent in each delay state by all connections. This is only available for connections with a TCP profile, not FastL4.

Click This	To View These Statistics
Connections	New and closed connections. It also shows mean connection length, measured from when Analytics starts collecting data (which may be from a mid-connection iRule) to when it stops.
Packets	Packets sent, packets received, and packets lost.

The system displays the different charts, and you can adjust the time period and view by settings on all the charts.

5. To save the charts to a PDF or to email the chart, click **Export** and specify the option to use.

   To use email, the BIG-IP system requires an SMTP server which you can configure at **System** > **Configuration** > **Device** > **SMTP**.

The TCP statistics are available to use for evaluating network performance. You can save the reports to track the differences in performance over time.

Sample TCP RTT statistics

This figure is a sample TCP statistics chart showing round trip times (RTT), or how long it takes for outgoing TCP packets on the client side to be answered by the server. When you hover over the chart, it shows the RTT minimum, RTT maximum, RTT average (mean), and the RTTVAR mean values. You can use these statistics to help gauge application performance.

Note: *To view RTT statistics for Layer 4 traffic managed using a FastL4 profile, you need to enable* ***RTT from Client*** *and* ***RTT from Server*** *(as appropriate) in the FastL4 profile.*

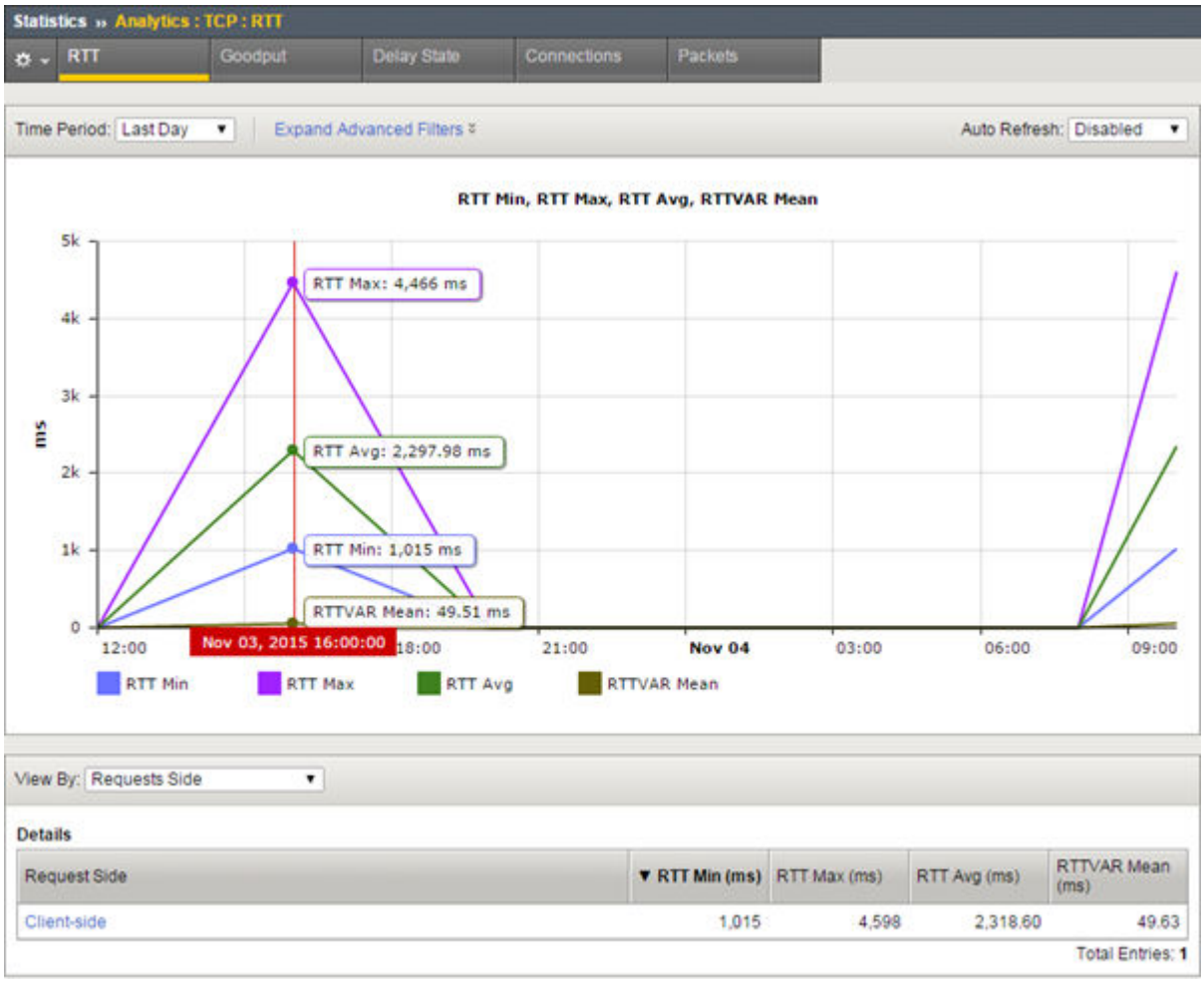


Figure 7: Sample TCP RTT statistics chart

Sample TCP goodput statistics

This figure is a sample TCP statistics report showing goodput sent and received values from the client side. Goodput shows throughput at the application level over a period of time. You can use these statistics to understand network performance.

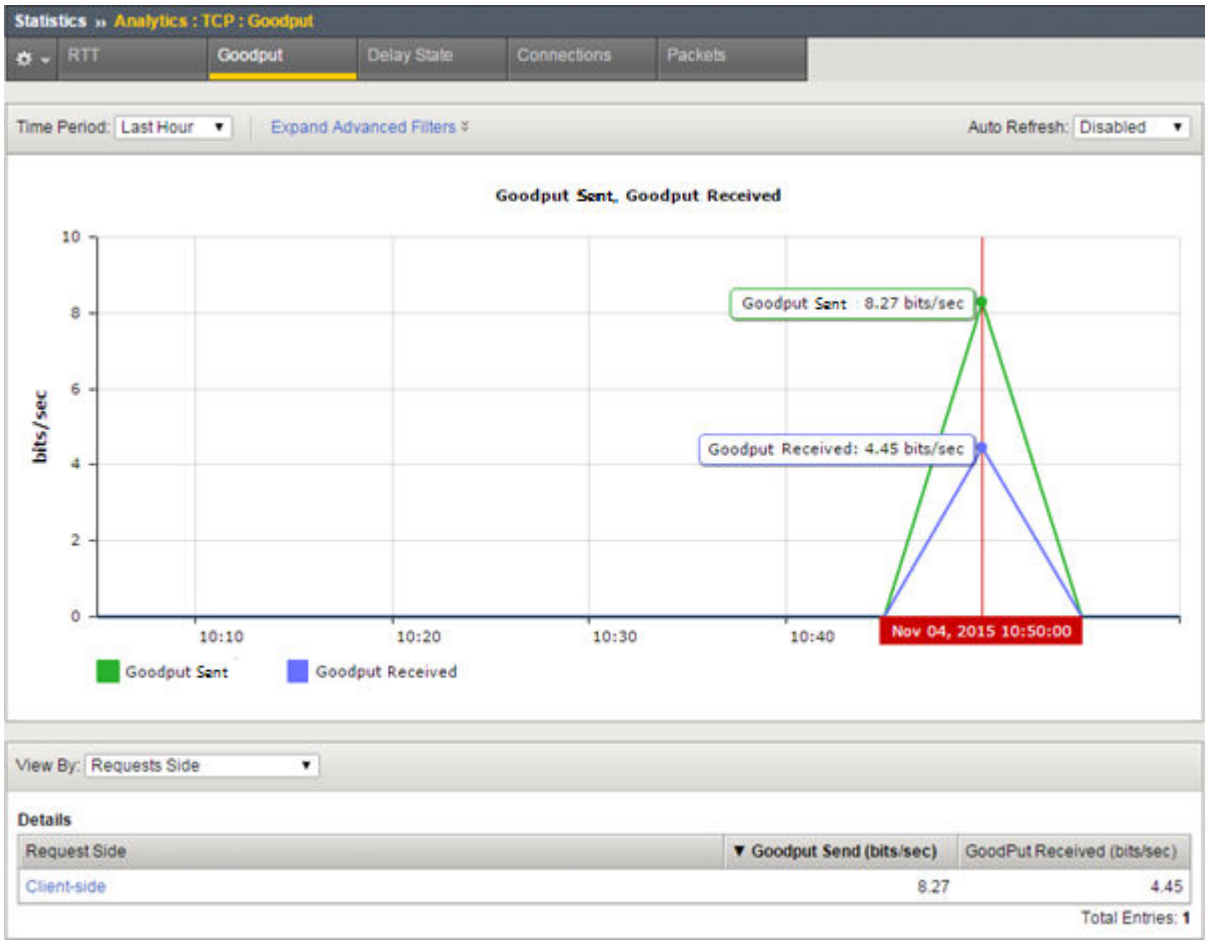


Figure 8: Sample TCP Goodput statistics chart

Sample TCP delay state statistics

This sample TCP statistics report shows the causes of delay states. Here the primary causes of delay are data in the congestion window, and waiting for the ACK.

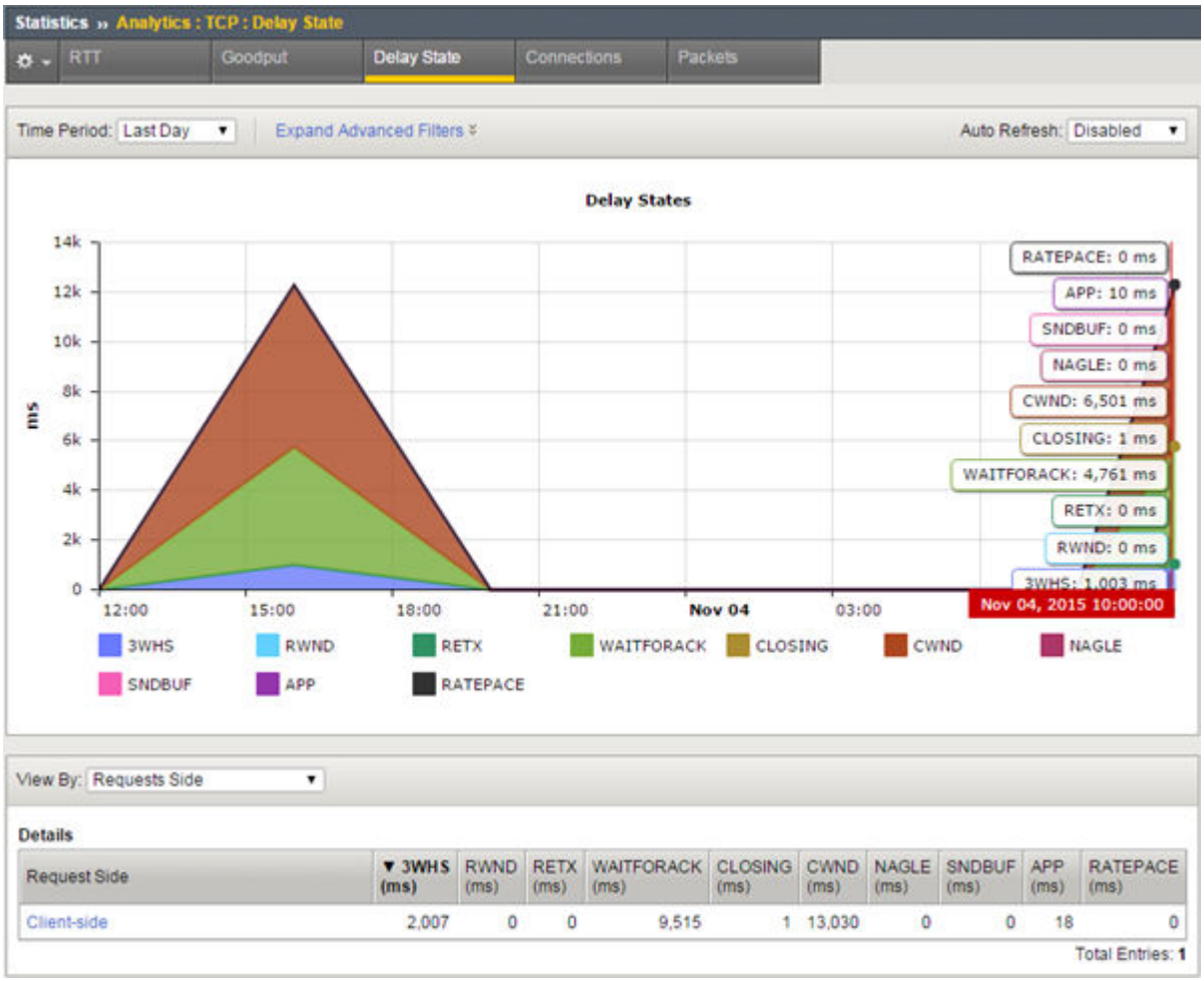


Figure 9: Sample TCP Delay State statistics chart

The delay states, described in the following table, are color coded in the chart. You can hover over the part of the chart you are interested in to display the delay states and their values. These states apply to outgoing data. Analytics picks the first listed state that matches the current situation.

State	Description and What to Do
3WHS	3-way handshake that starts a TCP connection. Analytics will accrue time in this state only if it can estimate the round-trip-time of the SYN or SYN-ACK that it sent.
RETX	Retransmission. TCP is resending data and/or waiting for acknowledgment of those retransmissions. This may indicate lossy links in the data path, or overly aggressive congestion control (for example, a profile with **Slow Start** disabled or improperly set **Packet Loss Ignore** settings). Activating rate-pace in the TCP profile may also help.
CLOSING	The BIG-IP® system has received acknowledgment of all data, sent the FIN, and is awaiting acknowledgement of the FIN. If the FIN goes out with the last chunk of data, you might not see this state at all. If there is a major issue on the client side, the issue may be that the servers are configured for *keepalive* (to not send FIN with their last data).

State	Description and What to Do
WAITFORACK	The BIG-IP system has sent all available data and is awaiting an ACK. If this state is prevalent, it could be a short connection, or possibly either the upper layers or the server are forcing TCP to frequently pause to accept new data.
APP	The BIG-IP system has successfully delivered all available data. There is a delay either at the client, the server, or in the layers above TCP on the BIG-IP system.
RWND	Receive-window limited. The remote host's flow-control is forcing the BIG-IP system to idle.
SNDBUF	The local send buffer settings limit the data in flight below the observed bandwidth/delay product. Correctable by increasing the **Send Buffer** size in the TCP profile.
CWND	Congestion-window limited. The TCP congestion window is holding available data. This is usually a legitimate response to the bandwidth-delay product and congestion on the packet path. In some cases, it might be a poor response to non-congestion packet loss (fixable using the **Packet Loss Ignore** profile options) or inaccurate data in the congestion metrics cache (addressable by disabling **Congestion Metrics Cache**, the ROUTE::clear iRule, or the `tmsh` command `delete net cmetrics dest-addr <addr>`).
NAGLE	TCP is holding sub-MSS size packets due to Nagle's algorithm. If the NAGLE state shows up frequently, disable **Nagle's algorithm** in the TCP profile.
RATEPACE	TCP is delaying transmission of packets due to rate pacing. This has no impact on achievable throughput, and no action is required.

Sample TCP connection statistics

This sample TCP connection report shows the average connection length in milliseconds, and the number of connections opened and closed during the last hour. If new connections are outpacing closed ones, that means the system may be unsustainably loaded.

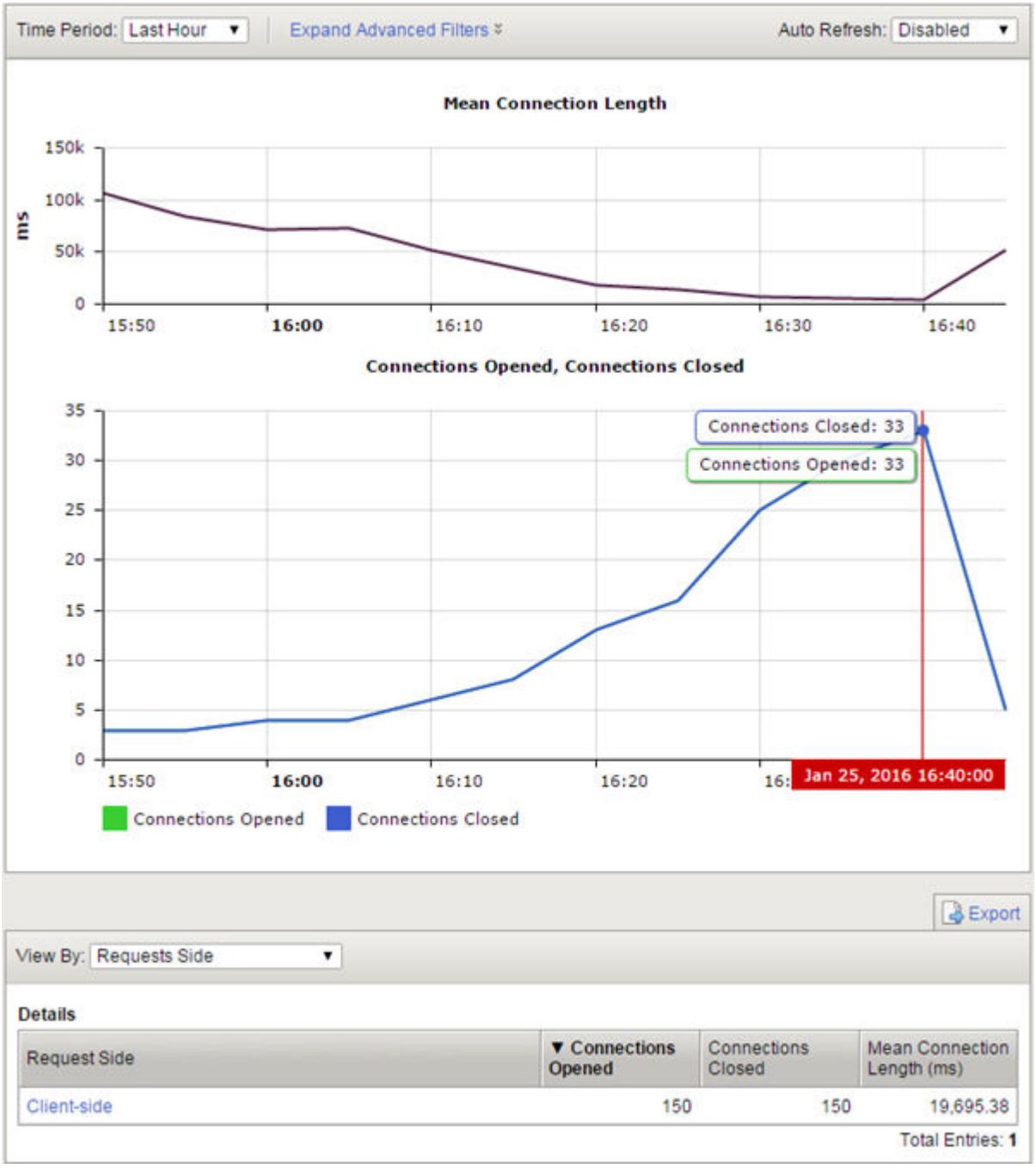


Figure 10: Sample TCP Connections statistics chart

You can change the information that is displayed in the chart and the Details table by changing the **View By** setting. For example, you can view by **Countries + Regions** to see where the connections are originating.

Sample TCP packets statistics

This sample TCP packets report shows the number of packets lost, sent, and received during the last hour. Packet loss is typically caused by network congestion, and can impact application performance.

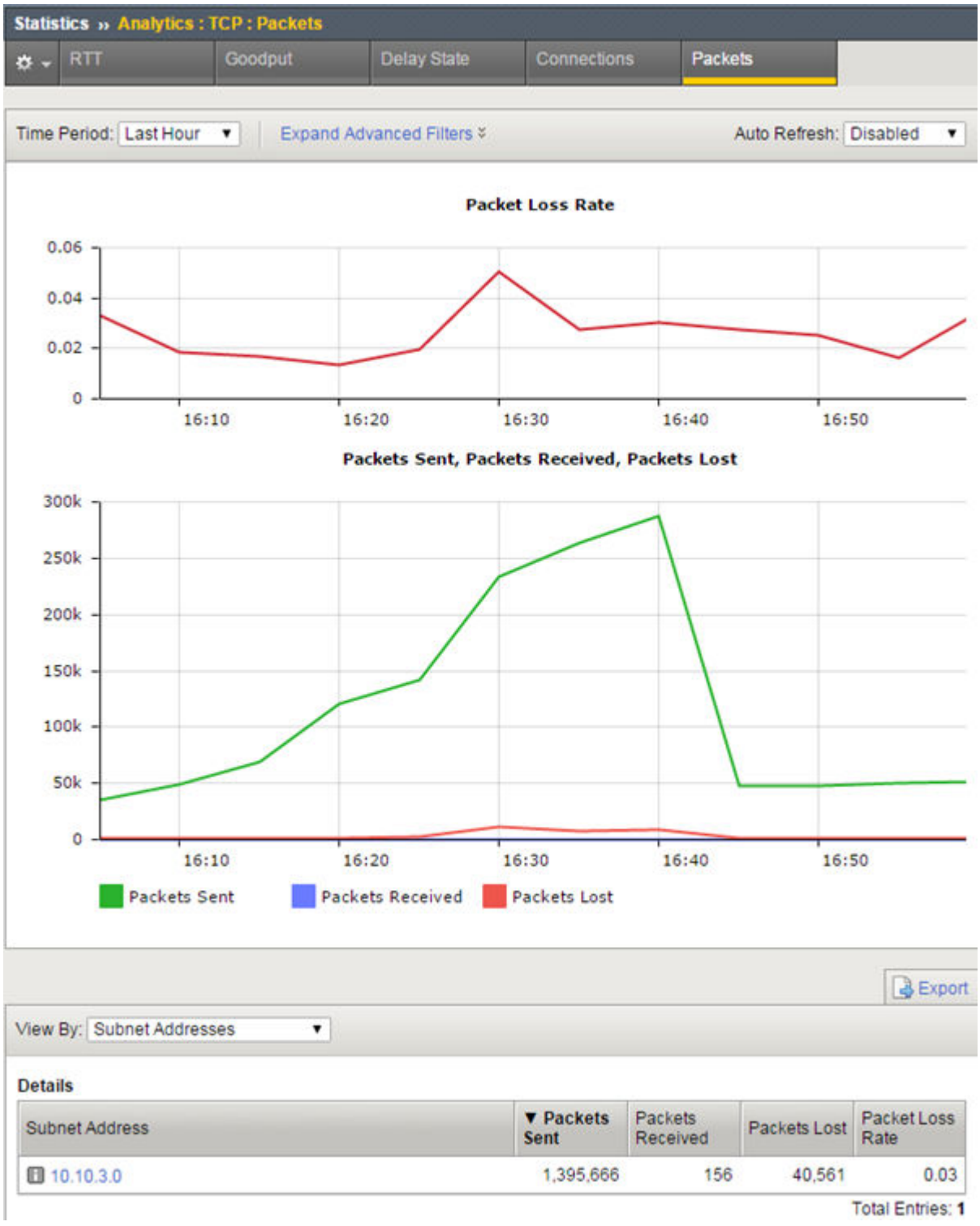


Figure 11: Sample TCP Packets statistics chart

You can drill down into the statistics. For example, on systems with multiple virtual servers, applications, or subnet addresses, you can investigate specific entities that might be having trouble. If users are having difficulties with an application, from the **View By** list, select **Applications**. In the Detail list, click the application to zoom in on the statistics for that application only.

Sample iRule for TCP Analytics

You can create a TCP Analytics profile that uses an iRule to collect the statistics. In the profile, for **Statistics Collection**, do not select either **Client Side** or **Server Side**. Let the iRule handle it.

For example:

```
# start collection for one subnet only.
  when CLIENT_ACCEPTED {
      if [IP::addr [IP::client_addr]/8 equals 10.0.0.0] {
        TCP::analytics enable
     }
  }
  when HTTP_REQUEST {
    # must check subnet again to avoid starting for all
    # connections
      if [IP::addr [IP::client_addr]/8 equals 10.0.0.0] {
       # make stats queryable by URI
         TCP::analytics key "[HTTP::uri]"
     }
  }
```

For more information about iRules®, refer to `devcentral.f5.com`.

Legal Notices

Legal notices

Publication Date

This document was published on November 13, 2017.

Publication Number

MAN-0357-10

Copyright

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.

Index

H

I

L

M

N

P

R

S

T

V