BIG-IP® Analytics: Implementations

Version 12.1

Table of Contents

Setting Up Application Statistics Collection

What is Analytics?

Analytics (also called Application Visibility and Reporting) is a module on the BIG-IP® system that you can use to visually analyze the performance of web applications, TCP traffic, FastL4, and overall system statistics. The statistics are displayed in graphical charts where you can drill down for more specific details to better understand network performance on certain devices, IP addresses, and so on. You can focus the statistics in the charts on different categories such as applications or virtual servers, depending on the chart.

For HTTP traffic, Analytics provides detailed metrics such as transactions per second, server and client latency, request and response throughput, and sessions. You can view metrics for applications, virtual servers, pool members, 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 categories, 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.

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, or with an iApps® application service. Each virtual server can have only one HTTP or 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.

Statistics > **Analytics** shows the HTTP Overview by default including the following sections (or widgets):

- Top virtual servers by average transactions per second
- Top URLs
- Top pool members by average transactions per second
- Top client subnets by average transactions per second
- Top response codes
- Top countries

Charts shown on the **Statistics** > **Analytics** screens include the application data saved for all HTTP Analytics profiles associated with iApps application services or virtual servers on the system. You can filter the HTTP information, for example, 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 values in the default profile so it includes the values you want it to have.

Certain information can only be specified 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: *If **Analytics** is not 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 only change the SMTP configuration 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 the statistics you want the system to collect:

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). In the Details table of the Analytics: HTTP Transactions screen, if you drill down into a specific entity, the system displays the maximum TPS. Drilling down in the Request Throughput details displays the maximum request throughput for each entity; and drilling down in the Response Throughput details displays the maximum response throughput for each entity.
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).

10. In the Statistics Gathering Configuration area, for **Collected Entities**, select the entities for which you want the system to collect statistics:

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 Analytics profile.
Response Codes	Saves HTTP response codes that the server returned to requesters.
User Agents	Saves information about browsers used when making the request.
Methods	Saves HTTP methods in requests.

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.

All other Analytics profiles you create inherit the values from the default Analytics profile. Statistics are collected for the virtual servers specified in this profile.

Collecting application statistics locally

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

Note: *Newer browsers (Internet Explorer 9 or later, Firefox 3.6 or later, or Chrome 14 or later) support viewing Analytics charts with no additional plug-in. If using older browsers (Internet Explorer 8 or earlier, Firefox 3.5 or earlier, or Chrome 13 or earlier), Adobe® Flash® Player (version 8 or later) must be installed on the computer where you plan to view Analytics charts.*

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. Select the **Custom** check box.
5. 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**.
6. You can use the default values for the rest of the General Configuration settings.
7. 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.

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

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). In the Details table of the Analytics: HTTP Transactions screen, if you drill down into a specific entity, the system displays the maximum TPS. Drilling down in the Request Throughput details displays the maximum request throughput for each entity; and drilling down in the Response Throughput details displays the maximum response throughput for each entity.
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).

10. In the Statistics Gathering Configuration area, for **Collected Entities**, select the entities for which you want the system to collect statistics:

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 Analytics profile.
Response Codes	Saves HTTP response codes that the server returned to requesters.
User Agents	Saves information about browsers used when making the request.
Methods	Saves HTTP methods in requests.

11. 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 the statistics you want the system to collect:

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). In the Details table of the Analytics: HTTP Transactions screen, if you drill down into a specific entity, the system displays the maximum TPS. Drilling down in the Request Throughput details displays the maximum request throughput for each entity; and drilling down in the Response Throughput details displays the maximum response throughput for each entity.
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.*

Option	Description
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).

12. In the Statistics Gathering Configuration area, for **Collected Entities**, select the entities for which you want the system to collect statistics:

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 Analytics profile.
Response Codes	Saves HTTP response codes that the server returned to requesters.
User Agents	Saves information about browsers used when making the request.
Methods	Saves HTTP methods in requests.

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: *If **Analytics** is not 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, including the following details:

- Overview
- Transactions
- Latency
- Throughput
- Sessions

The system updates the Analytics statistics every five minutes (you can refresh the charts periodically to see the updates). The Analytics Overview provides a summary of the most frequent recent types of application traffic, such as the top virtual servers, top URLS, top pool members, and so on. You can customize the Analytics Overview so that it shows the specific type of data you are interested in. You can also export the reports to a PDF file, or send the reports 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 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.

Note: *Newer browsers (Internet Explorer 9 or later, Firefox 3.6 or later, or Chrome 14 or later) support viewing Analytics charts with no additional plug-in. If using older browsers (Internet Explorer 8 or earlier, Firefox 3.5 or earlier, or Chrome 13 or earlier), Adobe® Flash® Player (version 8 or later) must be installed on the computer where you plan to view Analytics charts.*

You can review charts that show statistical information about traffic to your web applications. The charts provide visibility into application behavior, user experience, transactions, and data center resource usage.

1. On the Main tab, click **Statistics** > **Analytics** > **HTTP**.
   The Overview screen opens.
2. From the **Override time range to** list, select a new time frame to apply to all of the widgets in the overview.

   Tip: *Within each widget you can override the default time range, as needed.*

3. For each widget, select the data format and the time range to display, as needed.
4. From the menu bar, select the type of statistics you want to view.

Select this option	To see these application statistics
Overview	Top statistical information about traffic on your system or managed systems, such as the top virtual servers, top URLs accessed, and top applications. You can customize the information that is displayed.
Transactions	The HTTP transaction rate (transactions per second) passing through the web applications, and the number of transactions to and from the web applications.
Latency > Server Latency	The number of milliseconds it takes from the time a request arrives at the virtual server until a response arrives at the virtual server.
Latency > Page Load Time	The number of milliseconds it takes for a web page to fully load on a client browser, from the time the user clicks a link or enters a web address until the web page displays in its entirety.
Throughput > Request Throughput	HTTP request throughput in bits per second.
Throughput > Response Throughput	HTTP response throughput in bits per second.
Sessions > New Sessions	The number of transactions that open new sessions, in sessions per second.
Sessions > Concurrent Sessions	The total number of open and active sessions at a given time, until they time out.

The charts display information based on the settings you enabled in the HTTP Analytics profile.

5. From the **View By** list, select the specific network object type for which you want to display statistics.
   You can also click **Expand Advanced Filters** to filter the information that displays.
6. To focus in on the specific details you want more information about, click the chart or the details.
   The system refreshes the charts and displays information about the item.
7. On the screen, the system displays the path you followed to reach the current display, including the items you clicked. For example, to review throughput details for a particular virtual server, follow these steps:
   a) From the Throughput menu, choose Request Throughput.
   b) From the **View By** list, select **Virtual Servers**.
      The charts show throughput statistics for all virtual servers on this BIG-IP system. You can point on the charts to display specific numbers.
   c) Click the virtual server you want more information about. You can either click a part of the pie chart or click the name of the virtual server in the Details table.
      The charts show throughput statistics for that virtual server, and shows the path you used to display the information.
   d) To view information about other applications or retrace your path, click a link (in blue) in the path displayed by the charts.

   As you drill down into the statistics, you can locate more details and view information about a specific item on the charts.

You can continue to review the collected metrics on the system viewing transactions, latency, throughput, and sessions. As a result, you become more familiar with the system, applications, resource utilization, and more, and you can view the statistics in clear graphical charts, and troubleshoot the system as needed.

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.

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 the time period 12:35-13:35. By default, the BIG-IP® system displays one hour of data.

Exporting or emailing application statistics

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

You can export or email charts that show application statistics.

1. On the Main tab, click **Statistics** > **Analytics** > **HTTP**.
   The Overview screen opens.
2. Display the charts that show the information you want, clicking any of the menu bar options and adjusting the content as needed.
3. On the upper right of the charts screen, click **Export**.

   Tip: *You can also export any single report widget from the Overview screen. Click the widget configuration icon for the report and select* ***Export****.*

   The Choose Export Options popup screen opens.
4. Choose the appropriate option.
   - To save the report as a PDF on your computer, select **Save the report file on your computer**.
   - To send this report to someone, select **Send the report file via E-Mail as an attachment**, select the **SMTP Server**, and **Target E-Mail Address(es)**.
5. Click **Export**.
   The system saves the report to a file, or emails the file to the specified recipients. If SMTP is not configured (when sending reports by email), you receive a message that SMTP must be set up before you can send the reports.

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.

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 an iApps® application service.

Note: *Newer browsers (Internet Explorer 9 or later, Firefox 3.6 or later, or Chrome 14 or later) support viewing Analytics charts with no additional plug-in. If using older browsers (Internet Explorer 8 or earlier, Firefox 3.5 or earlier, or Chrome 13 or earlier), Adobe® Flash® Player (version 8 or later) must be installed on the computer where you plan to view Analytics charts.*

You can review statistics concerning server latency on the Analytics charts. *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.
2. From the Latency menu, choose Server Latency.
   A 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, in the Details table, select only that application.
   The charts show latency only for the selected application.
4. To view server latency for a specific virtual server:
   a) In the **View By** list, select **Virtual Servers**.
      The charts show latency for all virtual servers.
   b) In the Details list near the charts, click the virtual server you are interested in.
      The charts show latency only for the selected virtual server.
5. If further investigation is needed, in the **View By** setting, select other entities to view charts that show latency for other collected entities included in the Analytics profile, for example, specific pool members, URLs, countries, or client IP addresses.

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

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: *If **Analytics** is not 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 how long 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 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 Analytics charts. *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.
2. From the Latency menu, choose Page Load Time.
   Charts show the average page load times in milliseconds for all applications and virtual servers associated with all Analytics profiles.
3. To view average page load time for a specific application, in the Details table, select only that application.
   The charts refresh and show the page load time only for the selected application.
4. To view page load time for a specific virtual server:
   a) Click **Expand Advanced Filters**.
   b) For **Virtual Servers** select **Custom**.
   c) Click **Add** and select the virtual server whose page load times you want to view.

   The charts show page load times for the selected virtual server.
5. To zoom in on page load time during a specific time period, drag your cursor across the chart for the time period you are interested in.
   The system automatically refreshes the chart to display statistics for the time period you selected.

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 the statistics you want the system to collect:

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). In the Details table of the Analytics: HTTP Transactions screen, if you drill down into a specific entity, the system displays the maximum TPS. Drilling down in the Request Throughput details displays the maximum request throughput for each entity; and drilling down in the Response Throughput details displays the maximum response throughput for each entity.

Option	Description
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).

12. In the Statistics Gathering Configuration area, for **Collected Entities**, select the entities for which you want the system to collect statistics:

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 Analytics profile.
Response Codes	Saves HTTP response codes that the server returned to requesters.
User Agents	Saves information about browsers used when making the request.
Methods	Saves HTTP methods in requests.

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 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 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.

Note: *Newer browsers (Internet Explorer 9 or later, Firefox 3.6 or later, or Chrome 14 or later) support viewing Analytics charts with no additional plug-in. If using older browsers (Internet Explorer 8 or earlier, Firefox 3.5 or earlier, or Chrome 13 or earlier), Adobe® Flash® Player (version 8 or later) must be installed on the computer where you plan to view Analytics charts.*

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. Select the **Custom** check box.

5. 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**.

6. You can use the default values for the rest of the General Configuration settings.
7. 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.
8. In the Statistics Gathering Configuration area, select the **Custom** check box.
9. In the Statistics Gathering Configuration area, for **Collected Metrics**, select the statistics you want the system to collect:

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). In the Details table of the Analytics: HTTP Transactions screen, if you drill down into a specific entity, the system displays the maximum TPS. Drilling down in the Request Throughput details displays the maximum request throughput for each entity; and drilling down in the Response Throughput details displays the maximum response throughput for each entity.
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).

10. In the Statistics Gathering Configuration area, for **Collected Entities**, select the entities for which you want the system to collect statistics:

Option	Description
URLs	Collects the requested URLs.

Option	Description
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 Analytics profile.
Response Codes	Saves HTTP response codes that the server returned to requesters.
User Agents	Saves information about browsers used when making the request.
Methods	Saves HTTP methods in requests.

11. 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. 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**.
14. Click **Save** to add the rule to the local traffic policy.
15. To save the updated policy, click **Save Draft**.
    The Policy List Page opens.
16. 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, from the **Available** list, select the local traffic policy you previously created, 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 10 CPUs, all in use.

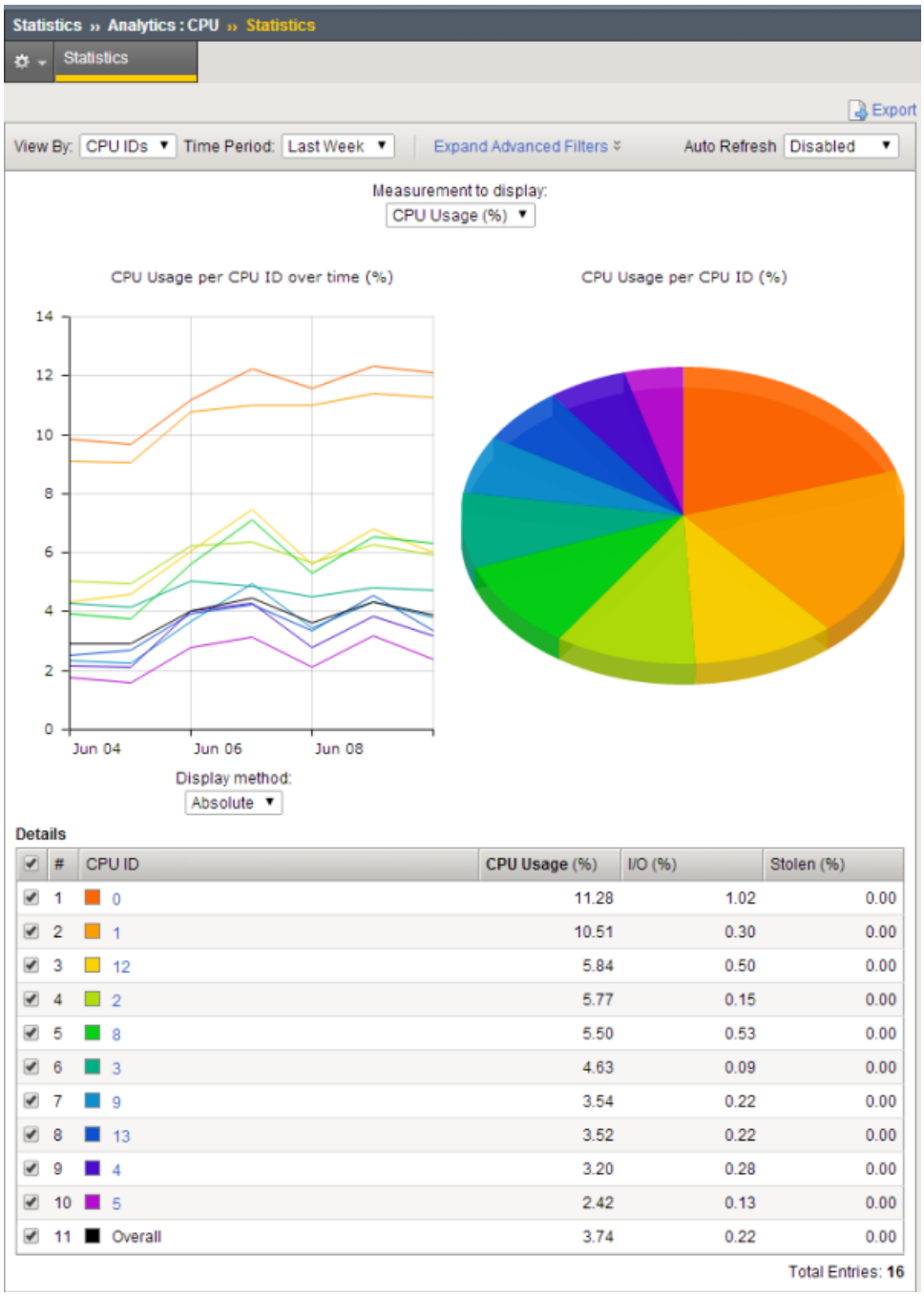


Figure 1: Sample CPU statistics

Sample system memory statistics

This figure shows a sample chart showing system RAM memory in use for the past day. This system has only one slot. On June 10 at 8:00 AM, average RAM went from 0 to 7.817 GB, probably when the system was started or when we sent some test traffic through the system.

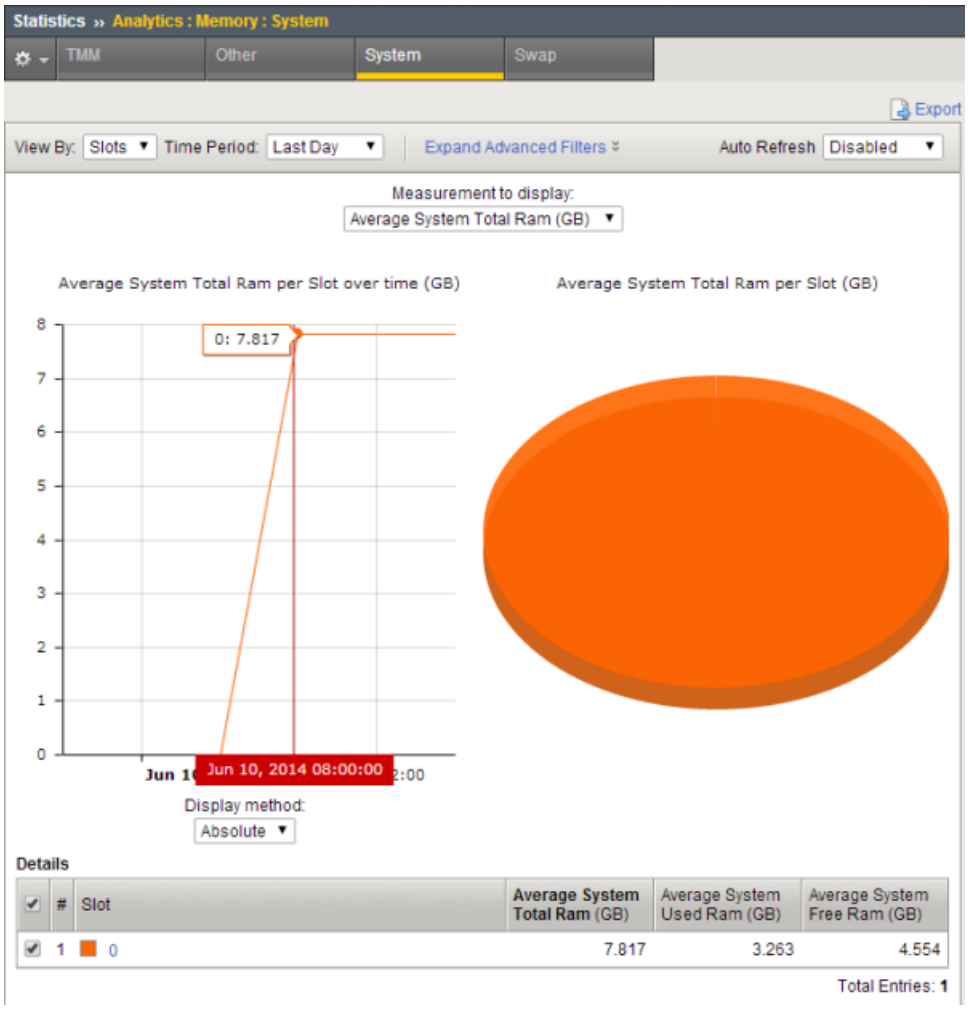


Figure 2: Sample system memory chart

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

Sample disk statistics

This figure shows a sample chart showing disk activity for the past hour. It shows that the total I/O activity on the system was 16753 I/O operations.

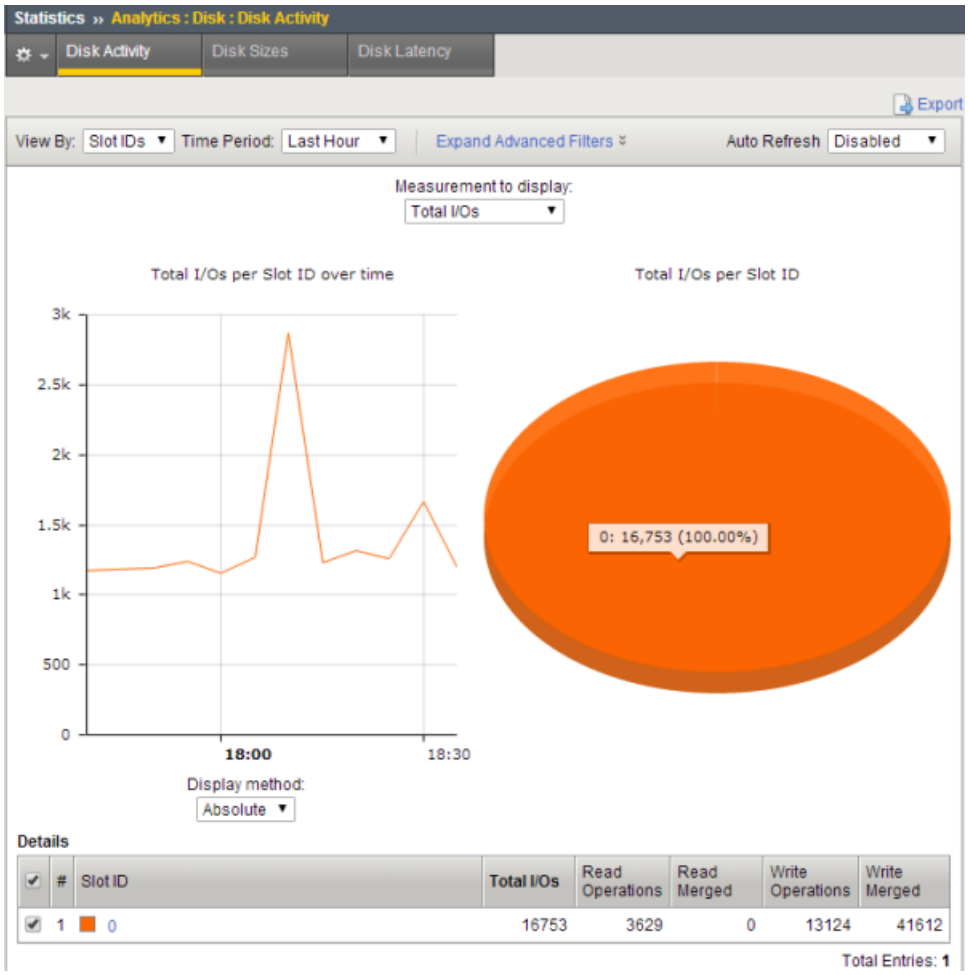


Figure 3: Sample Disk Activity chart

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.*

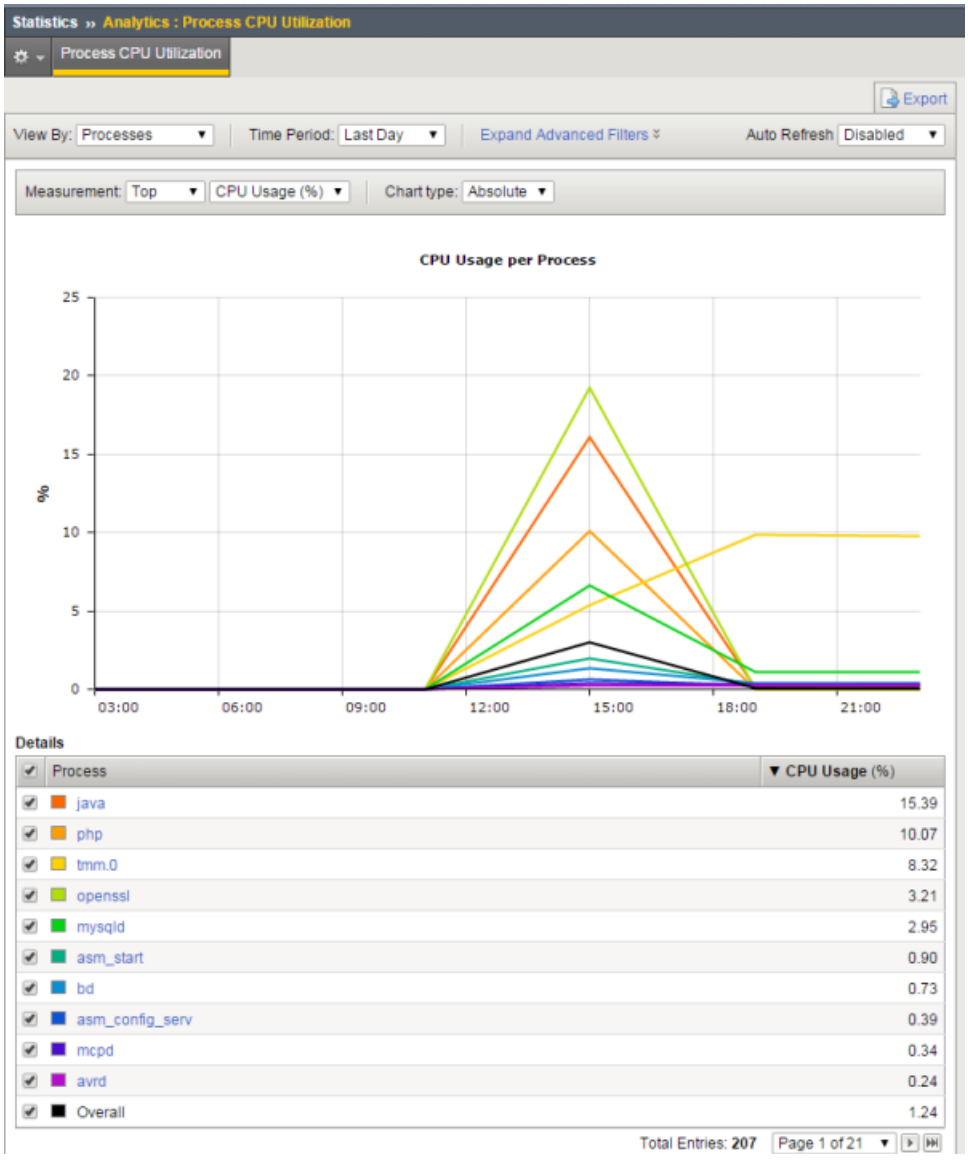
5. If you want to export the information in any of the charts, click **Export** and specify your options for how and where to send the data.

   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 figure shows a sample CPU usage report showing 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.



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.

Figure 4: Sample CPU statistics

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

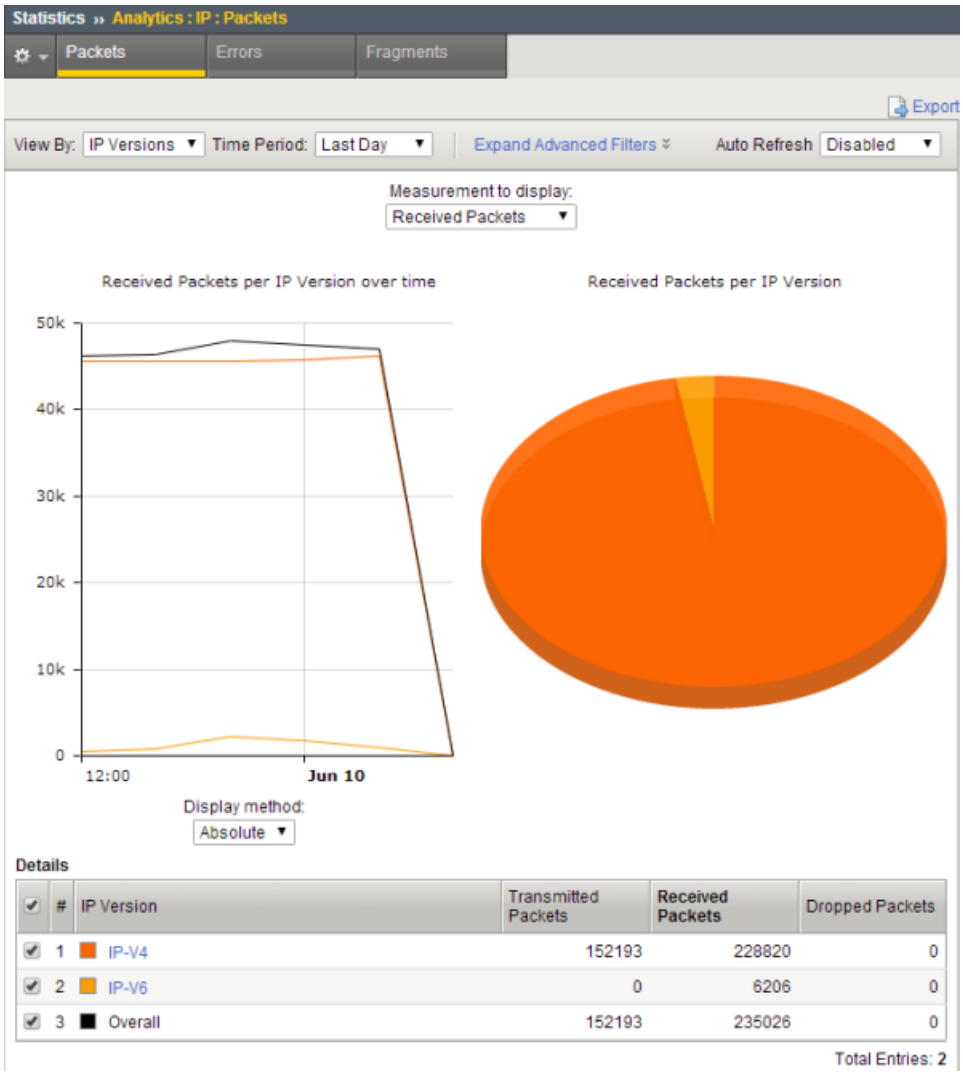
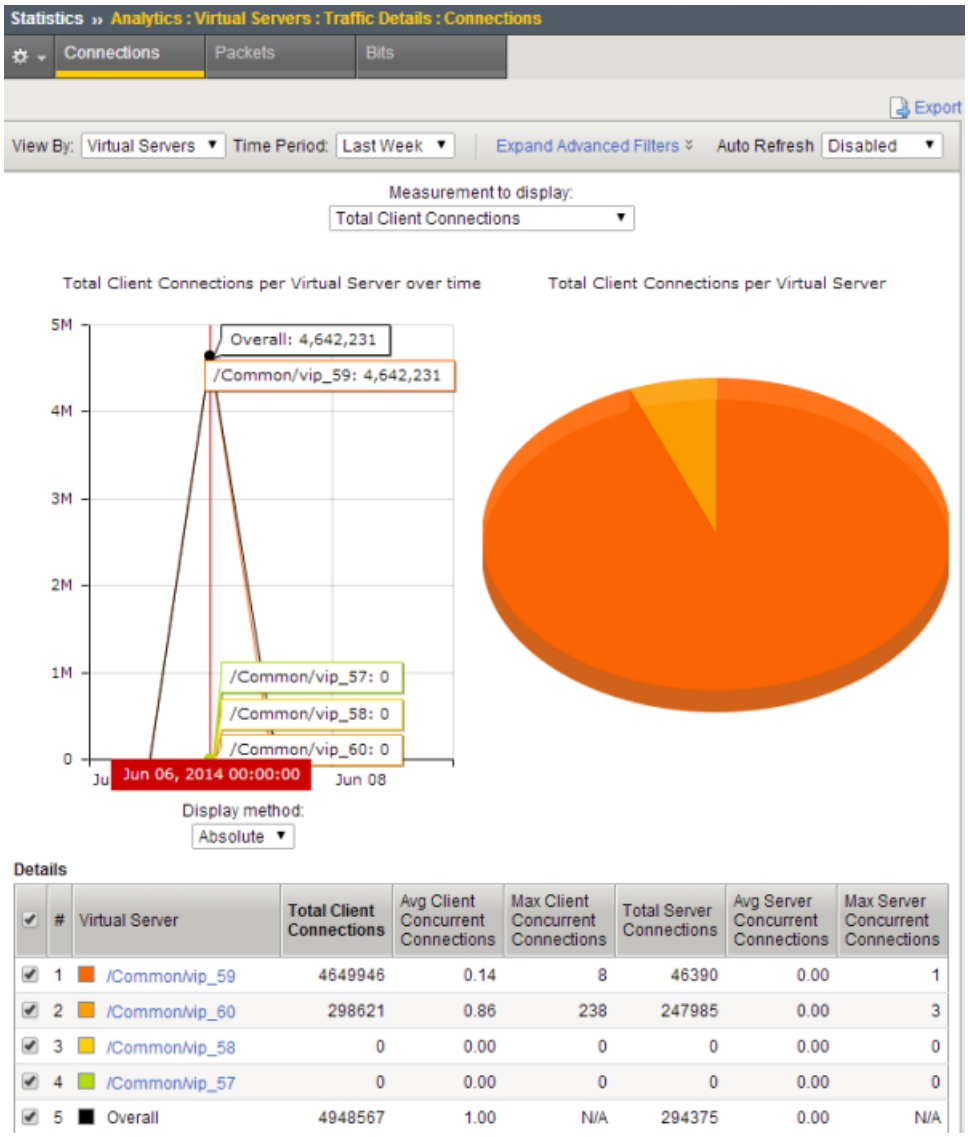


Figure 5: Sample IP Packets report

Sample Virtual Servers report

This figure shows a sample Virtual Servers report showing the number of client connections per virtual server. All of the traffic is on two of the virtual servers, `vip_59` and `vip_60`. By placing the cursor at the highest point, the screen shows details of the number of overall connections, the virtual server affected, and the time. This way you can monitor peak usage times.



	#	Virtual Server	Total Client Connections	Avg Client Concurrent Connections	Max Client Concurrent Connections	Total Server Connections	Avg Server Concurrent Connections	Max Server Concurrent Connections
☑	1	/Common/vip_59	4649946	0.14	8	46390	0.00	1
☑	2	/Common/vip_60	298621	0.86	238	247985	0.00	3
☑	3	/Common/vip_58	0	0.00	0	0	0.00	0
☑	4	/Common/vip_57	0	0.00	0	0	0.00	0
☑	5	Overall	4948567	1.00	N/A	294375	0.00	N/A

Figure 6: Sample Virtual Servers Traffic report

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.

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. 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. For **Statistics Collection**, leave the default, **Client side**, selected.

   This option specifies where the system gets the statistics from.
6. In the Associated Profiles 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.

7. 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.*

8. 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.

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.
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.

To collect RTT statistics for your Fast L4 virtual servers, verify that the RTT from client and/or the RTT from Server options are selected in your Fast L4 protocol profile (**Local Traffic** > **Profiles** > **Protocol** > **Fast L4** > **New Fast L4 Profile...**)

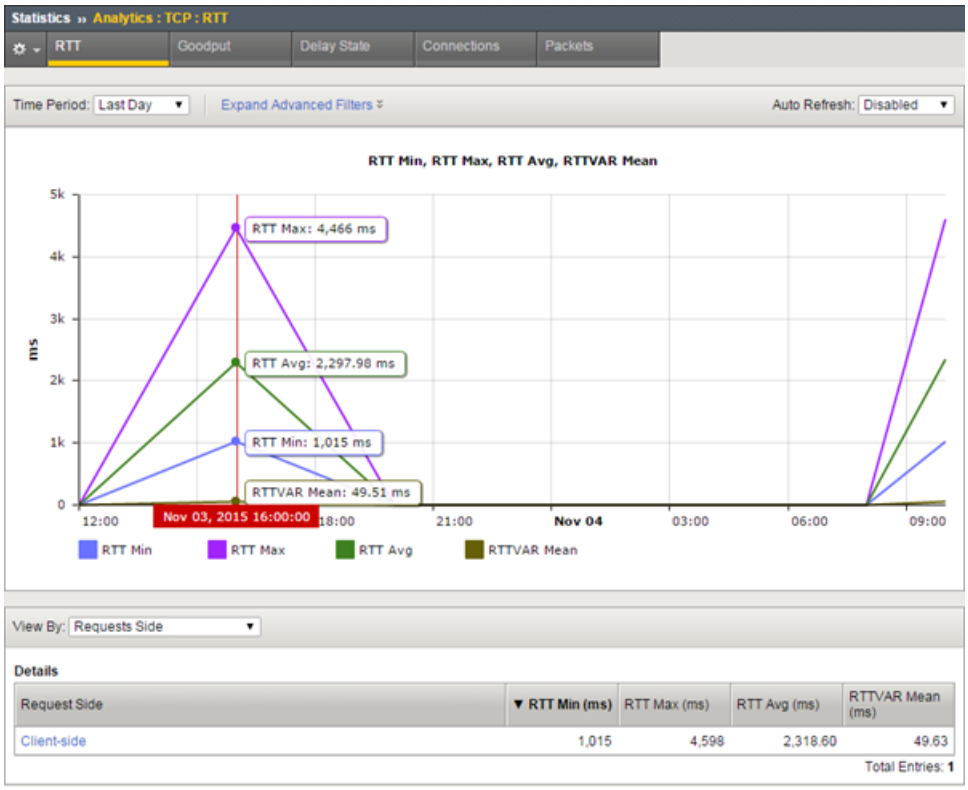


Figure 7: Sample TCP RTT statistics chart

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.

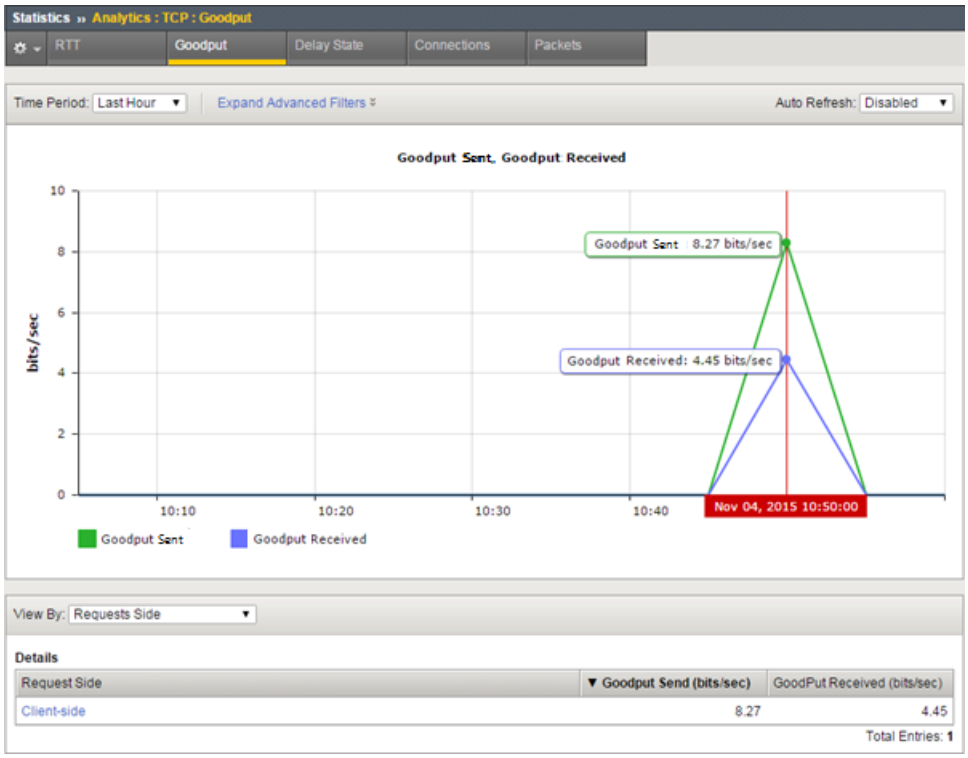


Figure 8: Sample TCP Goodput statistics chart

Sample TCP delay state statistics

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

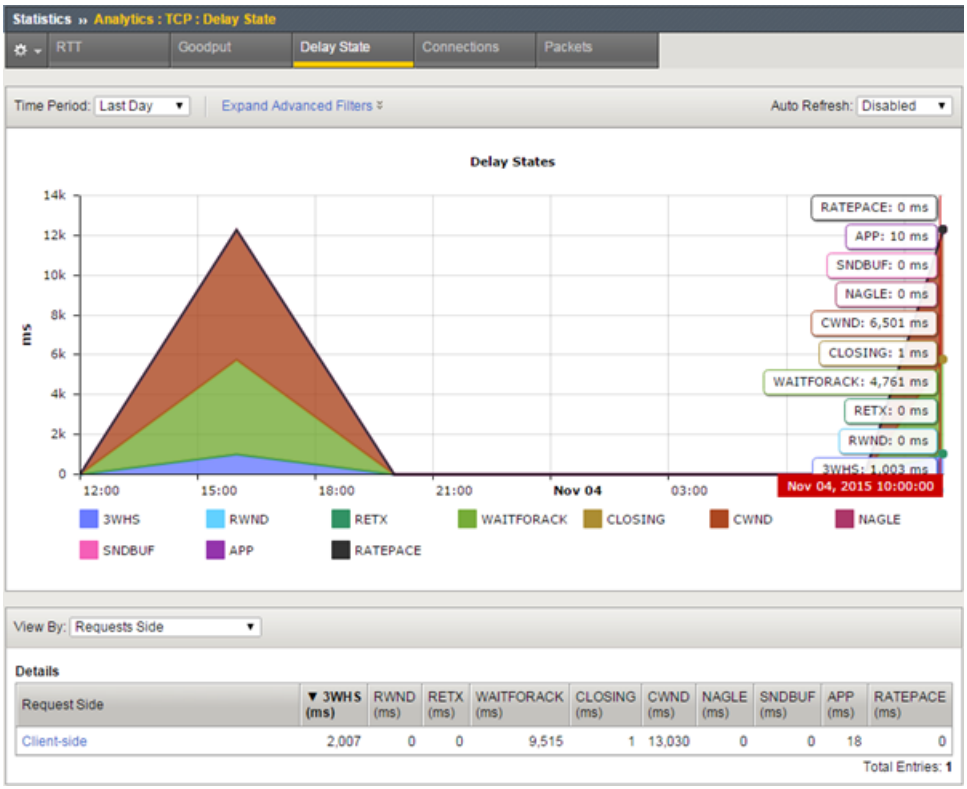


Figure 9: Sample TCP Delay State statistics chart

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).
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.

State	Description and What to Do
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 figure is a sample TCP connection report showing 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.

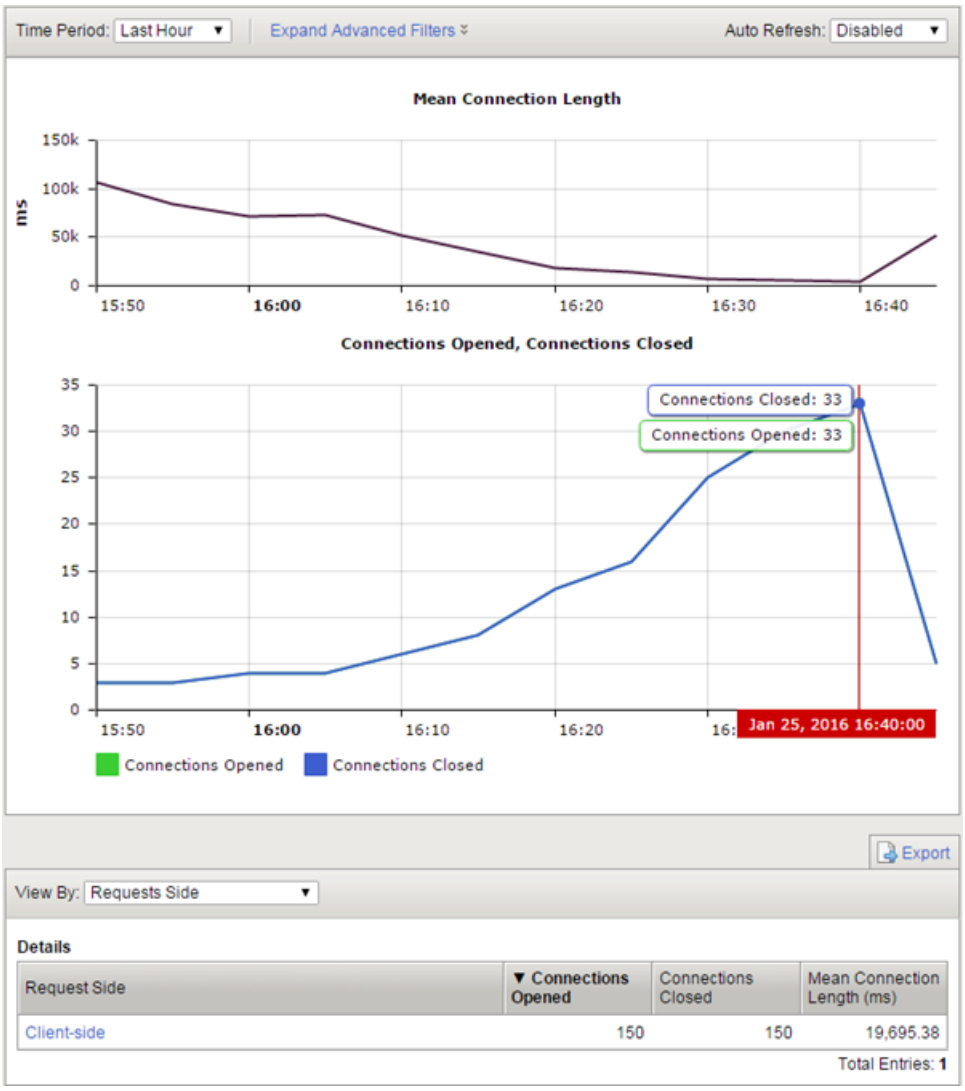


Figure 10: Sample TCP Connections statistics chart

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 figure is a sample TCP packets report showing 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.

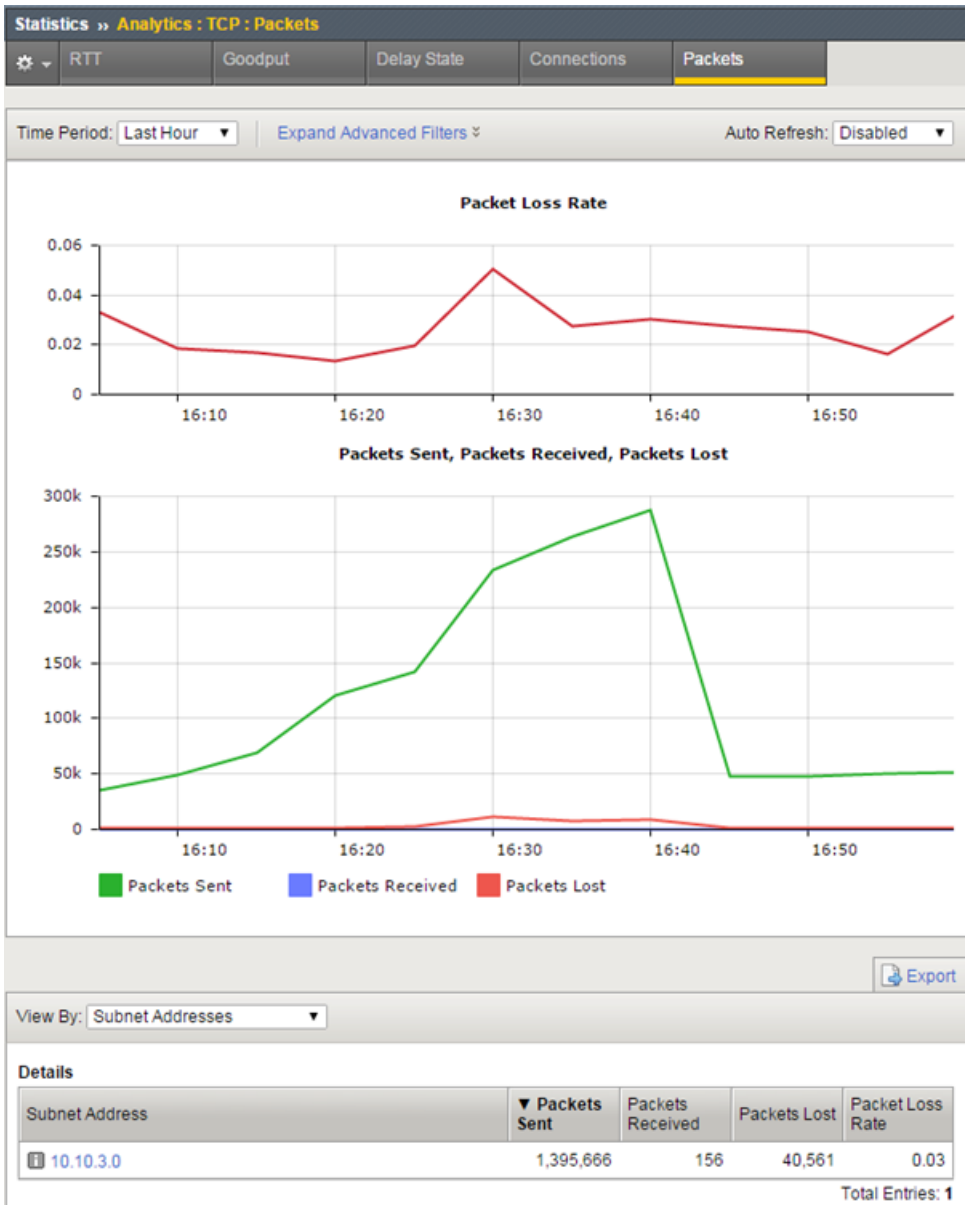


Figure 11: Sample TCP Packets statistics chart

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 January 10, 2018.

Publication Number

MAN-0357-08

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*

Link Controller Availability

This product is not currently available in the U.S.

Export Regulation Notice

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

RF Interference Warning

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

FCC Compliance

This equipment has been tested and found to comply with the limits for a Class A digital device pursuant to Part 15 of FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This unit generates, uses, and

can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case the user, at his own expense, will be required to take whatever measures may be required to correct the interference.

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

Canadian Regulatory Compliance

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

Standards Compliance

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

Index

L

M

N

P

R

S

T

V