BIG-IP® Analytics: Implementations

Version 11.2

IT agility. Your way.

Table of Contents

Table of Contents

Legal Notices

Publication Date

This document was published on May 7, 2012.

Publication Number

MAN-0357-02

Copyright

Trademarks

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.

Acknowledgments

This product includes software developed by Bill Paul.

This product includes software developed by Jonathan Stone.

This product includes software developed by Manuel Bouyer.

This product includes software developed by Paul Richards.

This product includes software developed by the NetBSD Foundation, Inc. and its contributors.

This product includes software developed by the Politecnico di Torino, and its contributors.

This product includes software developed by the Swedish Institute of Computer Science and its contributors.

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

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

This product includes software developed by Christopher G. Demetriou for the NetBSD Project.

This product includes software developed by Adam Glass.

This product includes software developed by Christian E. Hopps.

This product includes software developed by Dean Huxley.

This product includes software developed by John Kohl.

This product includes software developed by Paul Kranenburg.

This product includes software developed by Terrence R. Lambert.

This product includes software developed by Philip A. Nelson.

This product includes software developed by Herb Peyerl.

This product includes software developed by Jochen Pohl for the NetBSD Project.

This product includes software developed by Chris Provenzano.

This product includes software developed by Theo de Raadt.

This product includes software developed by David Muir Sharnoff.

This product includes software developed by SigmaSoft, Th. Lockert.

This product includes software developed for the NetBSD Project by Jason R. Thorpe.

This product includes software developed by Jason R. Thorpe for And Communications, http://www.and.com.

This product includes software developed for the NetBSD Project by Frank Van der Linden.

This product includes software developed for the NetBSD Project by John M. Vinopal.

This product includes software developed by Christos Zoulas.

This product includes software developed by the University of Vermont and State Agricultural College and Garrett A. Wollman.

This product includes software developed by Balazs Scheidler (bazsi@balabit.hu), which is protected under the GNU Public License.

This product includes software developed by Niels Mueller (nisse@lysator.liu.se), which is protected under the GNU Public License.

In the following statement, *This software* refers to the Mitsumi CD-ROM driver: This software was developed by Holger Veit and Brian Moore for use with 386BSD and similar operating systems. *Similar operating systems* includes mainly non-profit oriented systems for research and education, including but not restricted to NetBSD, FreeBSD, Mach (by CMU).

This product includes software developed by the Apache Group for use in the Apache HTTP server project (http://www.apache.org/).

This product includes software licensed from Richard H. Porter under the GNU Library General Public License (© 1998, Red Hat Software), www.gnu.org/copyleft/lgpl.html.

This product includes the standard version of Perl software licensed under the Perl Artistic License (© 1997, 1998 Tom Christiansen and Nathan Torkington). All rights reserved. You may find the most current standard version of Perl at http://www.perl.com.

This product includes software developed by Jared Minch.

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/).

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com).

This product contains software based on oprofile, which is protected under the GNU Public License.

This product includes RRDtool software developed by Tobi Oetiker (http://www.rrdtool.com/index.html) and licensed under the GNU General Public License.

This product contains software licensed from Dr. Brian Gladman under the GNU General Public License (GPL).

This product includes software developed by the Apache Software Foundation (http://www.apache.org/).

This product includes Hypersonic SQL.

This product contains software developed by the Regents of the University of California, Sun Microsystems, Inc., Scriptics Corporation, and others.

This product includes software developed by the Internet Software Consortium.

This product includes software developed by Nominum, Inc. (http://www.nominum.com).

This product contains software developed by Broadcom Corporation, which is protected under the GNU Public License.

This product contains software developed by MaxMind LLC, and is protected under the GNU Lesser General Public License, as published by the Free Software Foundation.

This product includes software developed by Ian Gulliver ©2006, which is protected under the GNU General Public License, as published by the Free Software Foundation.

Chapter 1

Setting Up Application Statistics Collection

Topics:

What is Analytics?

Analytics (also called Application Visibility and Reporting) is a module on the BIG-IP® system that you can use to analyze the performance of web applications. It 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 the traffic that is going through the system. You can capture traffic for examination and have the system send alerts so you can troubleshoot problems and immediately react to sudden changes.

The Analytics module also provides remote logging capabilities so that your company can consolidate statistics gathered from multiple BIG-IP appliances onto syslog servers or SIEM devices, such as Splunk.

About Analytics profiles

An *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. The Analytics module requires that you select an Analytics profile for each application you want to monitor. You associate the 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 Analytics profile associated with it.

In the 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 Analytics profile called **analytics**. It is a minimal profile that internally logs application statistics for server latency, throughput, response codes, and methods. You can modify the default profile, or create custom Analytics profiles for each application if you want to track different data for each one.

Charts shown on the **Statistics** > **Analytics** screens display the application data saved for all Analytics profiles associated with iApps application services or virtual servers on the system. You can filter the 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: Setting up application statistics collection

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 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

Following are tasks for setting up application collection.

Setting up local application statistics collection
Setting up remote application statistics collection
Configuring application performance alerts
Creating an SMTP configuration

Setting up local application statistics collection

You need to provision the Application Visibility and Reporting (AVR) module before you can set up local application statistics collection. You must have Adobe® Flash® Player installed on the computer where you plan to view Analytics statistics.

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

1. On the Main tab, click **Local Traffic** > **Profiles** > **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 Analytics screen opens and lists all Analytics profiles that are on the system, including a default profile called **analytics**.
2. Click **Create**.
   The New Analytics Profile screen opens. By default, the settings are initially the same as in the default **analytics** profile.
3. In the **Profile Name** field, type a name for the Analytics profile.
4. For the **Statistics Logging Type** setting, verify that **Internal** is selected. If it is not, select the check box on the right first to activate the setting, then select **Internal**.

   Selecting **Internal** causes the system to store statistics locally, and you can view the charts on the system by clicking **Overview** > **Statistics** > **Analytics**.
5. Review the read-only **Transaction Sampling Ratio** value, which shows the current global (analytics) status of sampling for the system.

   Learning from all transactions provides the most accurate statistical data but impacts performance. The system can perform traffic sampling; for example, sampling **1 of every 99** transactions; sampling is less precise but demands fewer resources. If you need to change the value, you can do it later by editing the default **analytics** profile.

   If using traffic sampling, the **Traffic Capturing Logging Type** setting and **User Sessions** metric option are not available.
6. In the Included Objects area, specify the virtual servers for which to capture application statistics:
   a) For the **Virtual Servers** setting, click **Add**.

A popup lists the virtual servers that you can assign to the Analytics profile.

b) From the Select Virtual Server popup list, select the virtual servers to include and click **Done**.

> ***Note:*** *You need to have previously configured the virtual servers (with an HTTP profile) for them to appear in the list. Also, you can assign only one Analytics profile to a virtual server so the list shows 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 a second one. In this case, you need to attach the Analytics profile to the second virtual server to ensure that the charts show accurate statistics.

7. To the right of the Statistics Gathering Configuration area, select the **Custom** check box.
The settings in the area become available for modification.
8. In the Statistics Gathering Configuration, for **Collected Metrics**, select the statistics you want the system to collect:

Option	Description
Server Latency	Tracks how long it takes to get data from the application server to the BIG-IP system (selected by default).
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.*
Throughput	Saves information about HTTP request and response throughput (selected by default).
User Sessions	Stores the number of unique user sessions. For **Timeout**, type the number of minutes of user non-activity to allow before the system considers the session to be over. If using transaction sampling, this option is not available.

9. 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 based on the client IP address.
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 **Trust XFF** is selected.
Response Codes	Saves HTTP response codes that the server returned to requesters (selected by default).
User Agents	Saves information about browsers used when making the request.
Methods	Saves HTTP methods in requests (selected by default).

10. Click **Finished**.
11. If you need to adjust the **Transaction Sampling Ratio** value, click the default **analytics** profile on the Profiles: Analytics screen.

You can use the sampling ratio to fine-tune the tradeoff between more accurate data and a possible performance impact. The value set here applies to all Analytics profiles on the system.

- Select **all** to collect all of the traffic that is being monitored and produce the most accurate results; it also poses the risk of performance reduction.
- Select **1 of every n** to sample every nth transaction; not all possible traffic is processed producing more generalized results, but performance is better.

Generally, it is best to use **all** when the BIG-IP system has low TPS, and use **1 of every n** when it has high TPS (for example, select **1 of every 20** to sample every twentieth request).

If you enable sampling (by selecting a setting other than **all**), the **User Sessions** metric and **Traffic Capturing Logging Type** settings become unavailable.

The BIG-IP system collects statistics about the application traffic described by the Analytics profile. You can view the statistics by clicking **Statistics** > **Analytics**.

If you want to monitor statistics for an iApps™ application, create the iApp application service, enable Analytics on the template, and specify the Analytics profile you just created. The BIG-IP system then collects statistics for the application service, and the application name appears in the Analytics charts.

Setting up remote application statistics collection

You need to provision the Application Visibility and Reporting (AVR) module: **System** > **Resource Provisioning** before you can set up remote application statistics collection. You also need the IP address and port number for the remote logging server.

You can configure the BIG-IP® system to collect application statistics remotely on syslog servers or SIEM devices, such as Splunk.

1. On the Main tab, click **Local Traffic** > **Profiles** > **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 Analytics screen opens and lists all Analytics profiles that are on the system, including a default profile called **analytics**.
2. Click **Create**.
   The New Analytics Profile screen opens. By default, the settings are initially the same as in the default **analytics** profile.
3. In the **Profile Name** field, type a name for the Analytics profile.
4. To the right of the General Configuration area, click the **Custom** check box.
   The settings in the area become available for modification.
5. For the **Statistics Logging Type** setting, click **External**.
6. For the **Remote Server IP Address** field, type the IP address of the external logging server.
7. For the **Remote Server Port** field, type the port used for the external logging server.
8. From the **Remote Server Facility** list, select the facility category of the logged traffic. The possible values are **LOG_LOCAL0** through **LOG_LOCAL7**.

   Tip: *If you configure remote logging for multiple applications, you can use the facility filter to sort the data for each.*

9. In the Included Objects area, specify the virtual servers for which to capture application statistics:

a) For the **Virtual Servers** setting, click **Add**.
A popup lists the virtual servers that you can assign to the Analytics profile.
b) From the Select Virtual Server popup list, select the virtual servers to include and click **Done**.

Note: *You need to have previously configured the virtual servers (with an HTTP profile) for them to appear in the list. Also, you can assign only one Analytics profile to a virtual server so the list shows 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 a second one. In this case, you need to attach the Analytics profile to the second virtual server to ensure that the charts show accurate statistics.

10. In the Statistics Gathering Configuration, for **Collected Metrics**, select the statistics you want the system to collect:

Option	Description
Server Latency	Tracks how long it takes to get data from the application server to the BIG-IP system (selected by default).
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.*
Throughput	Saves information about HTTP request and response throughput (selected by default).
User Sessions	Stores the number of unique user sessions. For **Timeout**, type the number of minutes of user non-activity to allow before the system considers the session to be over. If using transaction sampling, this option is not available.

11. 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 based on the client IP address.
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 **Trust XFF** is selected.
Response Codes	Saves HTTP response codes that the server returned to requesters (selected by default).
User Agents	Saves information about browsers used when making the request.
Methods	Saves HTTP methods in requests (selected by default).

12. 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.*

13. 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.

Configuring 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 e-mail 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**.

   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. For the **Statistics Logging Type**, ensure that the **Internal** check box is selected.

   If you also want external logging, click **External** and fill in the remote server fields.
4. 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.
5. For the **Notification Type** setting, select the appropriate check boxes to determine the type of notification and where you want to receive it:

To Send Alerts Like This	Do This
Local BIG-IP syslog (System > Logs > Local Traffic)	Select **Syslog**. The alerts are logged in the `/var/log/ltm` file.
Remote syslog server	Select **Syslog**. You must configure the remote syslog server on the BIG-IP system (refer to the BIG-IP documentation for details).
SNMP traps sent to an external SNMP receiver	Select **SNMP**. If you need to configure SNMP, wait until after you finish creating alerts. The system selects both **Syslog** and **SNMP**.
E-mail	Select **E-mail**. To send email alerts, you need to configure the BIG-IP system to communicate with a mail server.

6. 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) that 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.
7. Click **Update**.
8. 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**.
9. If you need to configure SMTP (if sending alerts by e-mail), click the default **analytics** profile on the Profiles: Analytics screen.
   a) For **SMTP Configuration**, select a 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 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 configuration

If you want the BIG-IP® system to send email or alerts, you need to create an SMTP server configuration.

1. On the Main tab, click **System** > **Configuration** > **Device** > **SMTP**.
2. Click **Create**.
   The New SMTP Configuration screen opens.
3. In the **Name** field, type a name for the SMTP configuration.
4. In the **SMTP Server Host Name** field, type the IP address or the fully qualified domain name (FQDN) of the SMTP server.

   If using the FQDN, make sure the DNS server is on the DNS lookup server list, and configure the DNS server on the BIG-IP system (**System** > **Configuration** > **Device** > **DNS**).
5. In the **SMTP Server Port Number** field, type the port number used for the SMTP server.

   Typically, the default SMTP port numbers are `25` (unencrypted or TLS), `465` (SSL encrypted), or `587` (TLS encrypted).
6. In the **Local Host Name** field, type the host name used in SMTP headers in the format of an FQDN; for example, `bigip.net`.

   This setting does not refer to the host name of the BIG-IP system.
7. In the **From Address** field, type the email address that the email is being sent from.

This is the address that the recipient sees. Because the BIG-IP system does not accept reply email, use either a valid email address or a from address such as `do-not-reply@bigip.net`.

8. To encrypt traffic between the BIG-IP system and the SMTP server, for **Encrypted Connection**, select the type of encryption, **SSL** (Secure Sockets Layer) or **TLS** (Transport Layer Security).
9. To require authentication on the SMTP server, for **Use Authentication**, select the **Enabled** check box, and type the user name and password.
10. Click **Finish**.

The SMTP configuration you created is now available for use. For example, you can use it when emailing statistics.

After you create the SMTP configuration, you need to specify it in the appropriate profile. You can create more than one SMTP configuration, if needed.

Chapter 2

Examining and Exporting Application Statistics

Topics:

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 or CSV file, or send the reports to one or more email addresses.

Note: *The displayed Analytics statistics are rounded up to two digits, and might be slightly inaccurate.*

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. To view Analytics statistics properly, you must have Adobe Flash Player installed on the computer where you plan to view them.

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**.
   The Analytics Overview screen opens.
2. Optionally, from the Time Period list (Last Hour, Last Day, Last Week, or Last Month) or the configuration gear settings for a widget, adjust the time range, data measurements, and format of data to display.
3. 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.

Select this option	To see these application statistics
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	How long it takes in milliseconds from the time a request arrives at the virtual server until a response arrives at the virtual server.
Latency > Page Load Time	How long it takes in milliseconds for a whole web page to fully load on a client's browser from the time the user clicks a link or enters a web address until the web page is completely displayed.
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 Analytics profile.

4. To view information specific to a particular network object type, select an option from the **View By** list.
   You can also click **Expand Advanced Filters** to filter the information that is displayed.
5. 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.
6. 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.

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**.
   The Analytics 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 Analytics Overview screen. Click the widget configuration icon for the report and select* ***Export****.*

   The Choose Export Options popup screen opens.
4. Select the appropriate options.

For this option	Do this
Export the data in *option* format	Specify the export format: • Select **PDF** to save the information in a graphical format to a PDF file. • Select **CSV (Time Series)** to export the information to a text file including specific information for time increments. • Select **CSV (Details Table)** to export the information to a text file providing summary details. If exporting the entire Overview screen, the information is saved only in PDF format (no export format options are available). When exporting widgets, the format options are **PDF** or **CSV** (only one CSV format is provided).
Save the report file on your computer	Select this option to save or open the file containing the report.
Send the report file as an attachment to the following E-mail address(es)	Type one or more email addresses (separated by comma or semicolon) to which to send the report.

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 configuration

If you want the BIG-IP® system to send email or alerts, you need to create an SMTP server configuration.

1. On the Main tab, click **System** > **Configuration** > **Device** > **SMTP**.
2. Click **Create**.
   The New SMTP Configuration screen opens.
3. In the **Name** field, type a name for the SMTP configuration.
4. In the **SMTP Server Host Name** field, type the IP address or the fully qualified domain name (FQDN) of the SMTP server.

   If using the FQDN, make sure the DNS server is on the DNS lookup server list, and configure the DNS server on the BIG-IP system (**System** > **Configuration** > **Device** > **DNS**).
5. In the **SMTP Server Port Number** field, type the port number used for the SMTP server.

   Typically, the default SMTP port numbers are `25` (unencrypted or TLS), `465` (SSL encrypted), or `587` (TLS encrypted).
6. In the **Local Host Name** field, type the host name used in SMTP headers in the format of an FQDN; for example, `bigip.net`.

   This setting does not refer to the host name of the BIG-IP system.
7. In the **From Address** field, type the email address that the email is being sent from.

   This is the address that the recipient sees. Because the BIG-IP system does not accept reply email, use either a valid email address or a from address such as `do-not-reply@bigip.net`.
8. To encrypt traffic between the BIG-IP system and the SMTP server, for **Encrypted Connection**, select the type of encryption, **SSL** (Secure Sockets Layer) or **TLS** (Transport Layer Security).
9. To require authentication on the SMTP server, for **Use Authentication**, select the **Enabled** check box, and type the user name and password.
10. Click **Finish**.

The SMTP configuration you created is now available for use. For example, you can use it when emailing statistics.

After you create the SMTP configuration, you need to specify it in the appropriate profile. You can create more than one SMTP configuration, if needed.

Chapter 3

Investigating Server Latency Issues

Topics:

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 Analytics profile that is logging statistics internally on the BIG-IP® system. In the profile, the statistics gathering configuration must have **Server Latency** selected as one of the collected metrics. The Analytics profile must be associated with one or more virtual servers, or an iApps™ application service. To view Analytics statistics properly, Adobe Flash Player must be installed on the computer where you plan to view them.

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**.
   The Analytics Overview screen opens.
2. From the Latency menu, click 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.*

Chapter 4

Viewing Application Page Load Times

Topics:

Overview: Viewing application page load times

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

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

- *Supports Navigation Timing by W3C*
- *Accepts cookies from visited application sites*
- *Enables JavaScript® for the visited application sites*

Viewing application page load times

Before you can view application page load times, you need to have created 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**.
   The Analytics 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** choose **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 mouse across the chart during 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.*

Chapter 5

Troubleshooting Applications by Capturing Traffic

Topics:

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. 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

Prerequisites for capturing application traffic

After you finish a basic networking configuration of the BIG-IP® system, you must complete the following tasks as 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.
- The **Traffic Sampling Ratio** must be set to **all** in the default Analytics profile.

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

Tip: *Before setting up traffic capturing, it is a good idea to clear the captured transaction log. On the Captured Transactions screen, click* ***Clear All*** *to clear all previously captured data records.*

Capturing traffic for troubleshooting

To set up traffic capturing, the **Transaction Sampling Ratio** of the default **analytics** profile must be set to **all**.

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 module.

Note: *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.*

1. On the Main tab, click **Local Traffic** > **Profiles** > **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 Analytics screen opens and lists all Analytics profiles that are on the system, including a default profile called **analytics**.
2. Click **Create**.
   The New Analytics Profile screen opens. By default, the settings are initially the same as in the default **analytics** profile.
3. In the **Profile Name** field, type a name for the Analytics profile.
4. To the right of the General Configuration area, click the **Custom** check box.
   The settings in the area become available for modification.
5. For **Traffic Capturing Logging Type**, specify where to store captured traffic.
   - To store traffic locally, click **Internal**. You can view details on the Statistics: Captured Transactions screen. This option is selected by default.
   - To store traffic on a remote logging server, click **External** and type the **Remote Server IP Address** and **Remote Server Port** number.

     Tip: *If you specify remote logging for multiple applications, you can use the **Remote Server Facility** filter to sort the data for each.*
6. In the Included Objects area, specify the virtual servers for which to capture application statistics:
   a) For the **Virtual Servers** setting, click **Add**.
      A popup lists the virtual servers that you can assign to the Analytics profile.
   b) From the Select Virtual Server popup list, select the virtual servers to include and click **Done**.

   Note: *You need to have previously configured the virtual servers (with an HTTP profile) for them to appear in the list. Also, you can assign only one Analytics profile to a virtual server so the list shows 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 a second one. In this case, you need to attach the Analytics profile to the second virtual server to ensure that the charts show accurate statistics.
7. In the Statistics Gathering Configuration, for **Collected Metrics**, select the statistics you want the system to collect:

Option	Description
Server Latency	Tracks how long it takes to get data from the application server to the BIG-IP system (selected by default).

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.*
Throughput	Saves information about HTTP request and response throughput (selected by default).
User Sessions	Stores the number of unique user sessions. For **Timeout**, type the number of minutes of user non-activity to allow before the system considers the session to be over. If using transaction sampling, this option is not available.

8. 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 based on the client IP address.
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 **Trust XFF** is selected.
Response Codes	Saves HTTP response codes that the server returned to requesters (selected by default).
User Agents	Saves information about browsers used when making the request.
Methods	Saves HTTP methods in requests (selected by default).

9. 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.

10. 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.*

11. 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 have created 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.

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 will help with troubleshooting 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.

Chapter 6

Viewing Application Statistics for Multiple Devices

Topics:

Overview: Viewing application statistics for multiple devices

You can use Enterprise Manager™ to view reports for managed devices that are provisioned to use Analytics, also referred to as Application Visibility and Reporting (AVR). The Enterprise Manager device must have an AVR centralized reporting license. You can display the Analytics reports for a single BIG-IP® device or aggregated reports for a group of devices. In this way, Enterprise Manager provides centralized Analytics reporting.

Analytics reports provide detailed metrics about application performance 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 one or more managed BIG-IP systems. With Enterprise Manager, you can create custom lists to view application statistics for only the devices you specify.

Viewing application statistics for multiple devices

Before you can use Enterprise Manager™ to view application statistics, one or more managed BIG-IP® devices needs to have Application Visibility and Reporting (AVR) provisioned. (The Enterprise Manager device does not need to have AVR provisioned but does require a centralized reporting license.) The managed devices each need to have an Analytics profile associated with one or more virtual servers, while collecting the type of data you specify locally. To view Analytics statistics properly, Adobe® Flash Player must be installed on the computer where you plan to view them.

With Enterprise Manager, you can view Analytics charts for one or more managed devices. The charts provide visibility into application behavior, user experience, transactions, and data center resource usage.

1. On the Main tab, click **Statistics** > **Analytics**.
   The Analytics Overview screen opens.
2. For each widget (or area on the screen), click the gear icon, and choose **Settings** to adjust what is displayed.

Setting	Description
Devices	Specifies a managed device or a list of managed devices for which you want to display statistics.
View all traffic by	Specifies type of data to view, and provides an optional filter so you can display more information.
Date range	Specifies the time period for which to display statistics (last hour, day, week, month).
Data visualization	Specifies how to format the data (details table, or line, pie, or bar chart).
Available measurements	Specifies up to six measurements to display in Details tables. Line, pie, or bar charts display only the first measurement.

3. 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.

Select this option	To see these application statistics
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	How long it takes in milliseconds from the time a request arrives at the virtual server until a response arrives at the virtual server.
Latency > Page Load Time	How long it takes in milliseconds for a whole web page to fully load on a client's browser from the time the user clicks a link or enters a web address until the web page is completely displayed.
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 Analytics profile.

4. To specify the devices for which to display application statistics, from the **Device(s)** list, select an option.
   - For multiple devices, select **Device list** and then select the name of a device list. ***All Devices**, provided by default, displays statistics for all managed BIG-IP devices (with AVR provisioned).
   - For one device, select **Device** and then select the name of the device.

Tip: *If you need to create custom device lists, click* ***Enterprise Management*** > ***Custom Lists****. On the Custom Lists screen, click* ***Create List****. Refer to online help for details about creating different types of custom device lists.*

5. To view information specific to a particular network object type, select an option from the **View By** list.
   You can also click **Expand Advanced Filters** to filter the information that is displayed.
6. To focus on specific information, click the chart or the details.
   The system refreshes the charts and displays specific information about the item.

You can use the collected metrics in the Analytics charts to view transactions, latency, throughput, and sessions for the managed systems provisioned with AVR. By examining the statistics in the charts, you can troubleshoot the systems more efficiently.

Index