BIG-IP® Analytics: Implementations

Version 11.0

IT agility. Your way.

Table of Contents

Legal Notices....5
Acknowledgments....7

Chapter 1: Setting Up Application Statistics Collection....9
What is Analytics?....10
About Analytics profiles....10
Overview: Setting up application statistics collection....10
Setting up local application statistics collection....11
Setting up remote application statistics collection....12
Configuring application performance alerts....14

Chapter 2: Examining Application Statistics....17
Overview: Examining application statistics....18
Examining application statistics....18

Chapter 3: Investigating Server Latency Issues....21
Overview: Investigating server latency issues....22
Investigating the server latency of applications....22

Chapter 4: Viewing Application Page Load Times....23
Overview: Viewing application page load times....24
Viewing application page load times....24

Chapter 5: Troubleshooting Applications by Capturing Traffic....27
Overview: Troubleshooting applications by capturing traffic....28
Prerequisites for capturing application traffic....28
Capturing traffic for troubleshooting....28
Reviewing captured traffic....30

Table of Contents

Legal Notices

Publication Date

This document was published on August 17, 2011.

Publication Number

MAN-0357-00

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.

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?*
- *About Analytics profiles*
- *Overview: Setting up application statistics collection*

What is Analytics?

Analytics (also called Application Visibility and Reporting) is a module on the BIG-IP® system that lets you analyze 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 create custom Analytics profiles for each application if you want to track different data for each one.

Charts shown in the **Overview** > **Statistics** > **Analytics** screen 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 click the tabs 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

Setting up local application statistics collection

You need to provision Application Visibility and Reporting (AVR): **System** > **Resource Provisioning** 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 application statistics locally. To do this, you create an Analytics profile to define which application performance statistics to collect. The BIG-IP system collects application performance statistics using the Application Visibility and Reporting module.

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 and you need to provision it first.*

   The Analytics screen opens and lists all Analytics profiles that are on the system.
2. Click **Create**.
   The New Analytics Profile screen opens.
3. In the **Profile Name** field, type a name for the Analytics profile.
   Names must begin with a letter, and can contain only letters, numbers, and the underscore (_) character.
4. In the Included Objects area, specify the virtual servers for which to capture performance 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 only virtual servers that have not been assigned an Analytics profile are listed.*
5. 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**.
6. To the right of the Statistics Gathering Configuration area, click the **Custom** check box.
   The settings in the area become available for modification.
7. For **Collected Metrics**, select the statistics you want the system to collect:

Options	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.
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 seconds for the maximum length of a session.

8. For **Collected Entities**, select the entities for which you want the system to collect statistics:

Options	Description
URLs	Collects the requested URLs.
Countries	Saves the name of the country where the request came from.
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 requestors (selected by default).
User Agent	Saves information about browsers used when making the request.
Methods	Saves HTTP methods in requests (selected by default).

9. Click **Finished**.

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

If you want to monitor statistics for an iApps™ application, create the iApps 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 Application Visibility and Reporting (AVR): **System** > **Resource Provisioning** before you can set up remote application statistics collection.

You can configure the BIG-IP® system to collect application statistics remotely on syslog servers or SIEM devices, such as Splunk. To do this, you create an Analytics profile to define which application performance statistics to collect. The BIG-IP® system collects application performance statistics using the Application Visibility and Reporting module.

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 and you need to provision it first.*

The Analytics screen opens and lists all Analytics profiles that are on the system.

2. Click **Create**.
   The New Analytics Profile screen opens.
3. In the **Profile Name** field, type a name for the Analytics profile.
   Names must begin with a letter, and can contain only letters, numbers, and the underscore (_) character.
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 **Statistics Logging Type**, click **External**.
6. For **Server IP Address**, type the IP address of the external logging server.
7. For **Server Port**, type the port used for the external logging server.
8. For **Remote Server Facility**, 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 performance 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 only virtual servers that have not been assigned an Analytics profile are listed.*

10. For **Collected Metrics**, click **Custom** then select the statistics you want the system to collect:

Options	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.
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 seconds for the maximum length of a session.

11. For **Collected Entities**, select the entities for which you want the system to collect statistics:

Options	Description
URLs	Collects the requested URLs.
Countries	Saves the name of the country where the request came from.
Client IP Addresses	Saves the IP address where the request originated.
Response Codes	Saves HTTP response codes that the server returned to requestors (selected by default).
User Agent	Saves information about browsers used when making the request.
Methods	Saves HTTP methods in requests (selected by default).

12. 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).

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 may 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.
4. 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**. The system selects **Syslog**, **SNMP** and **E-mail**. To send email alerts, you need to configure the BIG-IP system to communicate with a mail exchange server. Refer to Solution 3667 on the AskF5™ Knowledge Base web site, `support.f5.com`.

5. 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 above **100** and **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.
6. Click **Update**.
7. If SNMP is not configured on the BIG-IP system and you want to send SNMP traps or e-mail notifications, 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**.

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.

Chapter 2

Examining Application Statistics

Topics:

- *Overview: Examining application statistics*
- *Examining application statistics*

Overview: Examining application statistics

This implementation describes how to view application statistics on the BIG-IP® system. You can examine the statistics on the Analytics charts when Application Visibility and Reporting (AVR) is provisioned. The system recalculates the Analytics statistics and updates the charts every five minutes.

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, the template provided allows you to associate the virtual server. To view Analytics statistics properly, Adobe Flash Player must be 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 **Overview** > **Statistics** > **Analytics**.
   The Statistics: Analytics screen opens and shows charts with application statistics.
2. From the **Time Period** list (on the right), select the amount of time (last hour, day, week, or month) for which you want to view the statistics.

   Tip: *To display reports for a specific time period, for the* ***View*** *setting, select* ***Advanced****. In the* ***Time Period*** *list, you can then select* ***Custom*** *and specify the beginning and end dates.*

3. From the menu bar, select the type of statistics you want to view.

Select this menu bar option	To see these application statistics
Transactions	Displays the Layer 7 transaction rate (transactions per second) passing through the web application, and the number of transactions to and from the web application.
Latency > Server Latency	Displays 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	Displays how long it takes in milliseconds from the time a client's browser sends a request until the client's browser finishes loading the response.
Throughput > Request Throughput	Displays HTTP request throughput in bits per second.
Throughput > Response Throughput	Displays HTTP response throughput in bits per second.
Sessions > New Sessions	Displays the number of transactions that open new sessions in sessions per second.

Select this menu bar option	To see these application statistics
Sessions > Concurrent Sessions	Displays the total number of open and active sessions at a given time, until they time-out.

The information in the charts depends on the settings you enabled in the Analytics profile.

4. Click the tab for the entity (Applications, Virtual Servers, Pool Members, and so on) for which you want to display statistics; for example, click URLs to display statistics for each requested URL.

Tip: *You can also use the* ***Advanced*** *view (top right) to filter the information that is displayed.*

5. Focus in on the specific details you want to examine by clicking the item you want more information about. Click the chart or the details.
   The system refreshes the charts and displays information about the item.
6. Above the charts, the system displays the path you followed to reach the current display, including the items you clicked. For example, to check throughput on a particular virtual server, follow these steps:
   a) From the Throughput menu, choose Request Throughput.
   b) Click the **Virtual Servers** tab.
      The charts show throughput statistics for all virtual servers on this BIG-IP system. You can point on the charts to get 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. Above the charts, the path is displayed.
   d) To view information about other applications or retrace your path, click a link (in blue) in the path above the charts.

   As you drill down into the statistics, you can locate more details and view information for a specific item on all of the tabs.

Continue to review the collected metrics on the system by clicking on the menu items and tabs. As a result, you will get more familiar with the system, applications, resource utilization, and more, and you can view the statistics in clear graphical charts.

Chapter 3

Investigating Server Latency Issues

Topics:

- *Overview: Investigating server latency issues*
- *Investigating the server latency of applications*

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 **Overview** > **Statistics** > **Analytics**.
   The Statistics: Analytics screen opens and shows charts with application statistics.
2. From the **Time Period** list (on the right), select the amount of time (last hour, day, week, or month) for which you want to view the statistics.

   Tip: *To display reports for a specific time period, for the **View** setting, select **Advanced**. In the **Time Period** list, you can then select **Custom** and specify the beginning and end dates.*

3. From the Latency menu, click Server Latency.
   A chart shows the server latency for all applications and virtual servers associated with all Analytics profiles.
4. 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.
5. To view server latency for a specific virtual server:
   a) Click the **Virtual Servers** tab.
      The charts show latency for all virtual servers.
   b) In the Total Average Server Latency chart on the right, click the virtual server you are interested in.
      The charts show latency only for the selected virtual server.
6. If further investigation is needed, click the other tabs on the Analytics screen to view charts that show latency for other collected entities selected 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*
- *Viewing application page load times*

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 the application users' systems. 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:*

- *Includes support for Navigation Timing by W3C*
- *Enables cookies acceptance 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, until the web page response from the application server finishes loading on the end user's system.

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

1. On the Main tab, click **Overview** > **Statistics** > **Analytics**.
   The Statistics: Analytics screen opens and shows charts with application statistics.
2. From the **Time Period** list (on the right), select the amount of time (last hour, day, week, or month) for which you want to view the statistics.

   Tip: *To display reports for a specific time period, for the **View** setting, select **Advanced**. In the **Time Period** list, you can then select **Custom** and specify the beginning and end dates.*
3. From the Latency menu, choose Page Load Time.
   Charts show the page load time in milliseconds for all applications and virtual servers associated with all Analytics profiles.
4. To view 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.
5. To view page load time for a specific virtual server:
   a) Click the **Virtual Servers** tab.
      The charts show page load times for all virtual servers.

b) In the Total Average Page Load Time chart on the right, click the virtual server you are interested in.
The charts show page load time only for the selected virtual server.

6. To view information for a narrower time frame, click on a time in the left chart and drag it to the right chart.
The statistics now show information for a narrower time frame.
7. If further investigation is needed, click the other tabs on the Analytics screen to view charts that show page load times for other collected entities selected in the Analytics profile, for example, specific pool members, URLs, countries, or client IP addresses.

Tip: *If you are concerned about users' 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*

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.

The system logs the first 1000 transactions and displays charts based on the analysis of those transactions. To see additional application statistics, you can clear the existing data to display additional statistics.

Task Summary

Prerequisites for capturing application traffic
Capturing traffic for troubleshooting
Reviewing captured traffic

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 (**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 traffic locally or remotely (or both).

Capturing traffic for troubleshooting

You can configure the BIG-IP® system to capture application traffic 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 and you need to provision it first.*

   The Analytics screen opens and lists all Analytics profiles that are on the system.
2. Click **Create**.

The New Analytics Profile screen opens.

3. In the **Profile Name** field, type a name for the Analytics profile.
   Names must begin with a letter, and can contain only letters, numbers, and the underscore (_) character.
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.

Options	Description
Internal	Stores traffic locally and you can view details on the Statistics: Captured Transactions screen. This option is selected by default.
External	Stores traffic on a remote logging server if one is already configured on your network. If you select this check box, configure the **Remote Server IP Address** and **Server Port** number.

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

6. In the Included Objects area, specify the virtual servers for which to capture performance 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 only virtual servers that have not been assigned an Analytics profile are listed.*

7. 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.

Options	Description
None	Specifies that the system does not capture request (or response) data.
Header	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.

8. Depending on the application, customize the remaining filter settings to capture the portion of traffic to use for troubleshooting.

> ***Tip:*** *Focusing in on the data by limiting the type of information that is captured lets you 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.*

9. Click **Finished**.

The BIG-IP system captures the application traffic described by the Analytics profile for 1000 transactions (or until system limits are reached).

> ***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 internally. 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 **Overview** > **Statistics** > **Captured Transactions**.
   The Captured Transactions screen opens and lists all of the captured transactions.
2. Optionally, use the Filter settings to limit which transactions are listed. For each setting you want change, perform these steps:
   a) Click **Only**.
   b) Click the adjacent field.
      A popup window opens listing items (that is, applications, virtual servers, pool members, and so on) from the captured traffic.
   c) Select the item whose traffic you want to examine.
3. In the Captured Traffic area, click any transaction that you want to examine.
   Details of the request display on the screen below.
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, may 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 the previously captured data and start collecting transactions again.
   The system captures up to 1000 transactions and displays them on the screen. Captured transactions are visible approximately 10 seconds after they occur.

Index

A

alerts
    setting up application performance 14
analytics
    creating profiles for capturing traffic 28
    creating remote profiles 12
    setting up alerts 14
Analytics
    about 10
    capturing traffic overview 28
    creating profiles 11
    examining application statistics 18
    examining statistics overview 18
    investigating server latency 22
    investigating server latency overview 22
    prerequisites for traffic capture 28
    reviewing captured traffic 30
    setting up 10
    viewing page load times 24
    viewing page load times overview 24
Analytics profiles
    about 10
application monitoring
    about Analytics 10
application performance statistics
    capturing traffic overview 28
    setting up 10
application statistics
    collecting locally 11
    collecting remotely 12
    examining 18
    examining overview 18
    setting up alerts 14
application traffic capture
    prerequisites 28
Application Visibility and Reporting
    capturing traffic overview 28
    setting up 10
Application Visibility and Reporting (AVR)
    See also Analytics
    capturing traffic 28
    examining application statistics 18
    examining statistics overview 18
    investigating server latency 22
    investigating server latency overview 22
    reviewing captured traffic 30
    See Analytics 28
    setting up for remote statistics collection 12
    viewing page load times 24
    viewing page load times overview 24
        See also Analytics

C

captured traffic
    reviewing 30

L

latency
    investigating server 22

M

monitoring applications
    about Analytics 10

N

notifications
    setting up application performance 14

P

page load times
    viewing 24
profiles
    about Analytics 10
    creating Analytics 11
    creating analytics for capturing traffic 28
    creating remote analytics 12

S

server latency
    investigating 22
setting up for local statistics collection 11
statistics
    examining application 18

T

traffic
    capturing application 28
    capturing using Analytics 28
    reviewing captured 30
troubleshooting
    capturing application traffic 28
    investigating server latency 22
    reviewing captured traffic 30
    viewing page load times 24
troubleshooting applications 28
troubleshooting tactics for applications 10