BIG-IP® Analytics: Implementations

Version 11.5

Table of Contents

Legal Notices

Publication Date

This document was published on August 25, 2015.

Publication Number

MAN-0357-05

Copyright

Trademarks

Patents

This product may be protected by one or more patents indicated at:
http://www.f5.com/about/guidelines-policies/patents

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 Intel QuickAssist kernel module, library, and headers software licensed under the GNU General Public License (GPL).

This product includes software licensed from Gerald Combs (gerald@wireshark.org) under the GNU General Public License as published by the Free Software Foundation; either version 2 of the License, or any later version. Copyright ©1998 Gerald Combs.

This product includes software developed by Thomas Williams and Colin Kelley. Copyright ©1986 - 1993, 1998, 2004, 2007

Permission to use, copy, and distribute this software and its documentation for any purpose with or without fee is hereby granted, provided that the above copyright notice appear in all copies and that both that copyright notice and this permission notice appear in supporting documentation. Permission to modify the software is granted, but not the right to distribute the complete modified source code. Modifications are to be distributed as patches to the released version. Permission to distribute binaries produced by compiling modified sources is granted, provided you

1. distribute the corresponding source modifications from the released version in the form of a patch file along with the binaries,

2. add special version identification to distinguish your version in addition to the base release version number,
3. provide your name and address as the primary contact for the support of your modified version, and
4. retain our contact information in regard to use of the base software.

Permission to distribute the released version of the source code along with corresponding source modifications in the form of a patch file is granted with same provisions 2 through 4 for binary distributions. This software is provided "as is" without express or implied warranty to the extent permitted by applicable law.

This product contains software developed by Google, Inc. Copyright ©2011 Google, Inc.

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

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.

This product includes software developed by Jeremy Ashkenas and DocumentCloud, and distributed under the MIT license. Copyright © 2010-2013 Jeremy Ashkenas, DocumentCloud.

This product includes gson software, distributed under the Apache License version 2.0. Copyright © 2008-2011 Google Inc.

This product includes Boost libraries, which are distributed under the Boost license (http://www.boost.org/LICENSE_1_0.txt).

Chapter 1

Setting Up Application Statistics Collection

What is Analytics?

Analytics (also called Application Visibility and Reporting) is a module on the BIG-IP® system that you can use to 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 serves as the parent of all other Analytics profiles that you create on the system. 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** > **HTTP** 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

Changing the default values in the Analytics profile

The Application Visibility and Reporting (AVR) module includes a default analytics profile. You can edit the values in the default profile so it includes the values you want it to have.

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

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

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

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

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

   You can only change the SMTP configuration in the default profile. It is used globally for the system.
5. For the **Notification Type** setting, select how you want the system to send alerts and notifications.

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

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

6. If you want the system to perform traffic sampling, make sure the **Transaction Sampling** check box is selected.

   You can change this setting only in the default profile.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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.

Note:

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

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

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

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.

2. Click **Create**.
   The New Analytics profile screen opens.
3. In the **Profile Name** field, type a unique name for the Analytics profile.
4. Select the **Custom** check box.
5. For the **Statistics Logging Type** setting, verify that **Internal** is selected. If it is not, select it.

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

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

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

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

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

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

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

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

11. Click **Finished**.

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

Setting up remote application statistics collection

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

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

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

   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.
2. Click **Create**.
   The New Analytics profile screen opens.
3. In the **Profile Name** field, type a unique name for the Analytics profile.
4. Select the **Custom** check box.
5. For the **Statistics Logging Type** setting, select the **External** check box.
   The Publisher setting displays, below the **Traffic Capturing Logging Type** setting.
6. If you want the system to capture traffic, for the **Traffic Capturing Logging Type** setting, specify whether to store the traffic locally or on a remote server.

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

When you select the traffic capturing logging type, the screen displays the Capture Filter area, where you can indicate exactly what information to sample and log.

7. From the **Publisher** list, select the publisher that includes the destination to which you want to send log messages.

Tip: *Refer to External Monitoring of BIG-IP® Systems: Implementations for details.*

---

8. If you want the system to send email notifications, review the **SMTP Configuration** field to ensure that a configuration is specified and not the value **None**.

   You can configure SMTP only in the default Analytics profile. If it is not configured, you can save the profile and edit the default profile where you can select an existing SMTP configuration or create a new one. (If you click the **analytics** link without saving the new profile you are working on, you will lose the unsaved changes.)

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

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

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

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

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

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

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

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

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

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

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

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

14. Click **Finished**.

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

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 email alerts, the default **analytics** profile must specify an SMTP configuration.

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

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

---

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

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

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

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

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

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

   When you select a notification type, the screen displays the Alerts and Notifications Configuration area, where you can indicate the criteria for alerts and notifications.
7. In the Alerts and Notifications Configuration area, for the **Add New Rule** setting, define the rules that determine when the system sends alerts. Note that you cannot add overlapping rules, for example, two rules that request an alert when average TPS is greater than **100** and greater than **50** for **200** seconds.

a) For **Alert when**, select the condition under which you want to send an alert.
b) Select **below** or **above**, type an integer that represents the threshold value, and type the number of seconds (an integer, `300` or greater,) during which the rule has to apply.
c) Select the granularity level to which the threshold applies: traffic sent to an **Application**, a **Virtual Server**, or a **Pool Member**.
d) Click **Add**.
The rule is added to the list of Active Rules.

Continue to add as many rules as you want to specify conditions under which you want to be alerted.

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

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

Creating an SMTP server configuration

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

1. On the Main tab, click **System** > **Configuration** > **Device** > **SMTP**.
2. Click the **Create** button.
   The New SMTP Configuration screen opens.
3. In the **Name** field, type a name for the SMTP server that you are creating.
4. In the **SMTP Server Host Name** field, type the fully qualified domain name for the SMTP server host.
5. In the **SMTP Server Port Number** field, type a port number.
   For no encryption or TLS encryption, the default is `25`. For SSL encryption, the default is `465`.
6. In the **Local Host Name** field, type the host name used in the SMTP headers in the form of a fully qualified domain name.
   This host name is not the same as the BIG-IP system's host name.
7. In the **From Address** field, type the email address that you want displayed as the reply-to address for the email.
8. From the **Encrypted Connection** list, select the encryption level required for the SMTP server.
9. To require that the SMTP server validates users before allowing them to send email, select the **Use Authentication** check box, and type the user name and password required to validate the user.
10. Click the **Finish** button.

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

Chapter 2

Examining and Exporting Application Statistics

Overview: Examining and exporting application statistics

This implementation describes how to view application statistics on the BIG-IP® system. It describes how you can examine the statistics in the Analytics charts when Application Visibility and Reporting (AVR) is provisioned. Analytics charts display statistical information about traffic on your system, including the following details:

- Overview
- Transactions
- Latency
- Throughput
- Sessions

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

Note:

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

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

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

   Tip: *Within each widget you can override the default time range, as needed.*
3. For each widget, select the data format and the time range to display, as needed.
4. From the menu bar, select the type of statistics you want to view.

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

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

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

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

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

About the reporting interval for charts and reports

The system updates the statistics for charts and reports at five minute intervals: at five minutes after the hour, ten minutes after the hour, and so on.

Charts and data that you export from charts reflect the publishing interval of five minutes. For example, if you request data for the time period 12:40-13:40, the data in the chart or in the file that you export is for the time period 12:35-13:35. By default, the BIG-IP® system displays one hour of data.

Exporting or emailing application statistics

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

You can export or email charts that show application statistics.

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

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

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

Option	Action
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 server configuration

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

1. On the Main tab, click **System** > **Configuration** > **Device** > **SMTP**.
2. Click the **Create** button.
   The New SMTP Configuration screen opens.
3. In the **Name** field, type a name for the SMTP server that you are creating.
4. In the **SMTP Server Host Name** field, type the fully qualified domain name for the SMTP server host.
5. In the **SMTP Server Port Number** field, type a port number.
   For no encryption or TLS encryption, the default is `25`. For SSL encryption, the default is `465`.
6. In the **Local Host Name** field, type the host name used in the SMTP headers in the form of a fully qualified domain name.
   This host name is not the same as the BIG-IP system's host name.
7. In the **From Address** field, type the email address that you want displayed as the reply-to address for the email.
8. From the **Encrypted Connection** list, select the encryption level required for the SMTP server.
9. To require that the SMTP server validates users before allowing them to send email, select the **Use Authentication** check box, and type the user name and password required to validate the user.
10. Click the **Finish** button.

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

Chapter 3

Investigating Server Latency Issues

Overview: Investigating server latency issues

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

Investigating the server latency of applications

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

Note:

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

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

1. On the Main tab, click **Statistics** > **Analytics** > **HTTP**.
   The Overview screen opens.
2. From the Latency menu, choose Server Latency.
   A chart shows the server latency for all applications and virtual servers associated with all Analytics profiles.
3. To view server latency for a specific application, in the Details table, select only that application.
   The charts show latency only for the selected application.
4. To view server latency for a specific virtual server:
   a) In the **View By** list, select **Virtual Servers**.
      The charts show latency for all virtual servers.
   b) In the Details list near the charts, click the virtual server you are interested in.
      The charts show latency only for the selected virtual server.
5. If further investigation is needed, in the **View By** setting, select other entities to view charts that show latency for other collected entities included in the Analytics profile, for example, specific pool members, URLs, countries, or client IP addresses.

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

Chapter 4

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 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.

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

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

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

1. On the Main tab, click **Statistics** > **Analytics** > **HTTP**.
   The Overview screen opens.
2. From the Latency menu, choose Page Load Time.
   Charts show the average page load times in milliseconds for all applications and virtual servers associated with all Analytics profiles.
3. To view average page load time for a specific application, in the Details table, select only that application.
   The charts refresh and show the page load time only for the selected application.
4. To view page load time for a specific virtual server:
   a) Click **Expand Advanced Filters**.
   b) For **Virtual Servers** select **Custom**.
   c) Click **Add** and select the virtual server whose page load times you want to view.

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

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

Chapter 5

Troubleshooting Applications by Capturing Traffic

Overview: Troubleshooting applications by capturing traffic

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

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

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

Task Summary

Capturing traffic for troubleshooting
Reviewing captured traffic

About prerequisites for capturing application traffic

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

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

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

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

Capturing traffic for troubleshooting

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

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

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

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.

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

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

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

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

Option	Description
Max TPS and Throughput	Collects statistics showing the maximum number of transactions occurring per second and the amount of traffic moving through the system (maximum request and response throughput is collected and recorded separately). In the Details table of the Analytics: HTTP Transactions screen, if you drill down into a specific entity, the system displays the maximum TPS. Drilling down in the Request Throughput details displays the maximum request throughput for each entity; and drilling down in the Response Throughput details displays the maximum response throughput for each entity.
Page Load Time	Tracks how long it takes an application user to get a complete response from the application, including network latency and completed page processing. ***Note:*** *End-user response times and latencies can vary significantly based on geography and connection types.*

Option	Description
User Sessions	Stores the number of unique user sessions. For **Timeout**, select the number of minutes of user inactivity to allow before the system considers the session to be over. For **Cookie Secure Attribute**, specify whether to secure session cookies. Options are **Always**, the secure attribute is always added to the session cookie; **Never**, the secure attribute is never added to the session cookie; or **Only SSL**, the secure attribute is added to the session cookie only when the virtual server has a client SSL profile (the default value).

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

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

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

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

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

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

15. Click **Finished**.

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

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

Reviewing captured traffic

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

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

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

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

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

Chapter 6

Using Local Traffic Policies with Analytics

Overview: Using local traffic policies with Analytics

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

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

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

Task Summary

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.

Note:

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

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

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

   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.
2. Click **Create**.
   The New Analytics profile screen opens.
3. In the **Profile Name** field, type a unique name for the Analytics profile.
4. Select the **Custom** check box.
5. For the **Statistics Logging Type** setting, verify that **Internal** is selected. If it is not, select it.

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

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

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

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

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

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

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

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

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

11. Click **Finished**.

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

Creating a local traffic policy for Analytics

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

1. On the Main tab, click **Local Traffic** > **Policies** > **Policy List**.
   The Policy List screen opens.
2. Click **Create**.
   The New Policy screen opens.
3. In the **Name** field, type a unique name for the policy.
4. For the **Strategy**setting, select **first-match** to apply the actions in the first rule that matches.
5. For the **Requires** setting, select **http** from the **Available** list, and move the entry to the **Selected** list using the Move button.
6. For the **Controls** setting, select **avr** from the **Available** list, and move the entry to the **Selected** list using the Move button.

   This local traffic policy is specifically for controlling Analytics.
7. In the Rules area, click **Add** to create a rule that defines when traffic is handled by the security policy.
8. In the **Rule Name** field, type the word `index`.
9. In the Manage Conditions area, define the application traffic to which this rule applies. Specify the following values and use the default values for the rest.
   a) From the **Operand** list, select **http-uri**.
   b) From the **Selector** list, select **path**.
   c) From the **Condition** list, select **contains**; then, in the field below, type `index` and click **Add**.
   d) Click **Add Condition**.
10. In the Manage Actions area, define the action to apply to the traffic. Specify the following values and use the default values for the rest.
    a) From the **Target** list, select **avr**.
    b) From the **Action** list, select **disable**.
    c) Click **Add Action**.
11. Click **Finished** to add the rule to the local traffic policy.
    The policy properties screen opens.
12. Create a default rule that enables Analytics for all other traffic.

a) In the Rules area, click **Add**.
b) In the **Rule Name** field, type the word `default`.
c) Leave the default values for the **Condition** setting, which means apply this rule to traffic that does not meet the other rule.
d) From the **Target** list, select **avr**.
The system automatically sets **Event** to **request** and **Action** to **enable**, which are the settings we want to use in this case.
e) Click **Finished**.

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

Associating a local traffic policy with a virtual server

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

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

Implementation results

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

Chapter 7

Viewing Application Statistics for Multiple ASM Devices

Overview: Viewing analytics for multiple ASM devices

You can use Enterprise Manager™ to view reports for managed BIG-IP® Application Security Manager™ devices that are provisioned for Application Visibility and Reporting (AVR).

Analytics reports provide detailed metrics about application performance such as transactions per second, server and client latency, request and response throughput, and sessions. Metrics are provided for applications, virtual servers, pool members, URLs, specific countries, and additional detailed statistics about application traffic running through one or more managed devices. You can view the analytics reports for a single device, view aggregated reports for a group of devices, and create custom lists to view analytics for only specified devices. In this way, Enterprise Manager provides centralized analytics reporting.

Viewing analytics charts and data

Before you can use Enterprise Manager™ to view analytics, you must license it with the Centralized Analytics add-on key. If your web browser is IE8 or earlier, install Adobe® Flash Player on the system where you want to view the analytics. You must also provision the managed BIG-IP® Application Security Manager™ devices for Application Visibility and Reporting (AVR), and associate the analytics profile with one or more virtual servers.

Analytics provide visibility into application behavior, user experience, transactions, and data center resource usage. You can use this information to troubleshoot issues and to increase the efficiency of your network.

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

Setting	Description
View by	Specifies how you want to view the statistics, for example, by virtual server, URL, country, pool, and so on. It also 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).
Show details	Specifies the quantity of top level statistics to display.
Available measurements	Specifies up to six measurements to display in Details tables. Line, pie, or bar charts display only the first measurement that you select.
Data visualization	Specifies how to format the data (details table, or line, pie, or bar chart).

   These settings revert to the defaults when you change screens.
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.
Transactions	The HTTP transaction rate (transactions per second) passing through the web applications, and the number of transactions to and from the web applications.

Select this option	To see these application statistics
Latency > Server Latency	The number of milliseconds it takes from the time a request arrives at the virtual server until a response arrives at the virtual server.
Latency > Page Load Time	The number of milliseconds it takes for a web page to fully load on a client browser, from the time the user clicks a link or enters a web address until the web page displays in its entirety.
Throughput > Request Throughput	HTTP request throughput in bits per second.
Throughput > Response Throughput	HTTP response throughput in bits per second.
Sessions > New Sessions	The number of transactions that open new sessions, in sessions per second.
Sessions > Concurrent Sessions	The total number of open and active sessions at a given time, until they time out.

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

4. If using Enterprise Manager, you can 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 devices for which AVR is provisioned.
   - For one device, select **Device** and then select the name of the device.

Tip: *You also have the option to create a custom list of devices by clicking* ***Enterprise Management*** *>* ***Custom Lists*** *and on the Custom Lists screen, clicking* ***Create List****.*

---

5. From the **View By** list, select the specific network object type for which you want to display statistics.

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

6. To focus on specific information, click the chart or the details.

   The easiest way to learn more what is available is to experiment by clicking on the statistics screens and by viewing the data in various formats.

Index

T

V