CA Nimsoft Monitor

Probe Guide for Apache HTTP Server Monitoring

apache v1.5 series

Legal Notices

Contact CA

Contact CA Support

For your convenience, CA Technologies provides one site where you can access the information that you need for your Home Office, Small Business, and Enterprise CA Technologies products. At http://ca.com/support, you can access the following resources:

- Online and telephone contact information for technical assistance and customer services
- Information about user communities and forums
- Product and documentation downloads
- CA Support policies and guidelines
- Other helpful resources appropriate for your product

Providing Feedback About Product Documentation

Send comments or questions about CA Technologies Nimsoft product documentation to nimsoft.techpubs@ca.com.

To provide feedback about general CA Technologies product documentation, complete our short customer survey which is available on the CA Support website at http://ca.com/docs.

Contents

Documentation Changes

This table describes the version history for this document.

Version	Date	What's New?
1.5	September 2013	Initial web-based GUI version of this probe. (Previous versions of this probe are configured using Infrastructure Manager).

Chapter 1: Overview

The Apache HTTP Server Monitoring probe is used for remote (agentless) monitoring of the Apache HTTP servers. The Apache HTTP server is an open source software and supports numerous of hardware platforms and operating systems. The Apache HTTP server can maintain a high level of availability and performance to its user community. These features make it the most popular HTTP server for hosting numerous of business critical web Sites.

The Apache HTTP Server Monitoring probe has the following features:

- Centralized and agent less monitoring of multiple Apache HTTP servers.
- Monitoring the server level measures and response time for an individual Apache HTTP server.
- Monitoring of individual requested resources.
- Generating Quality of Service data for trend analysis.
- Monitoring the compliance with the Service Level Agreements.
- Detecting the server problems and degradations quickly.
- Identifying the bottlenecks and point of failure.
- Real-time alerting and proactive response for problems impacting the service.
- Minimizing the service downtime.

This section contains the following topics:

About This Guide

This guide is for the CA Nimsoft Monitor Administrator to help understand the configuration of the Apache HTTP Server Monitoring probe.

This guide contains the following information:

- An overview of the Apache HTTP Server Monitoring probe.
- The related documentation for previous probe versions, release notes, and so on.
- The configuration details of the probe including information for the fields that are required to configure the probe.
- The common procedures that can be used in the probe configuration.
- Field information for the fields with their default values.

Important! The field description for intuitive terms in the GUI has not been included in the document.

Related Documentation

For related information that may be of interest, see the following material:

Related Documentation

Documentation for other versions of the apache probe

The Release Notes for the apache probe

User documentation for the Admin Console

Monitor Metrics Reference Information for CA Nimsoft Probes (http://docs.nimsoft.com/prodhelp/en_US/Probes/ProbeReference/index.htm)

Preconfiguration Requirements

The Apache HTTP Server Monitoring probe requires certain configuration settings on the Apache Web servers. These settings allow the Apache Web servers to provide the performance and the extended status information to the Apache HTTP Server Monitoring probe.

Retrieving Performance from the Apache HTTP server

The probe retrieves performance data from the Apache HTTP server using HTTP to access the server-status URL of the server to be monitored.

The Apache HTTP server provides a module for reporting performance data over HTTP. The URL that directs to this page is "<server name>/server-status". You can view the sample output from the Web server of Apache.org, the organization behind the HTTP server.

Note: The *server-status* module must have been installed and configured on the Apache HTTP server to be monitored. The *server-status* module allows the computer hosting the monitoring probe to access the server-page.

Access the URL http://www.apache.org/server-status and it returns the verbose version of the status page. You can add the "?auto" at the end of the URL and access the less verbose version of the page; for example, http://www.apache.org/server-status?auto. The less verbose version is more suitable for programmatic use.

Note: The less verbose version does not return connection level details. Therefore, it is not possible to monitor individual resources using this option.

You can restrict access to authorized users or computers (the IP addresses), while configuring the server-status page. You can avoid the availability of the information to the intruders by restricting the access.

The *Extended Status* module must be installed on the Apache HTTP server for retrieving detailed worker thread information. A worker thread is used for handling individual requested resources. However, this option is not required to achieve the server level monitoring.

Note: All official documentation for the Apache HTTP server is available online and can be found here: http://httpd.apache.org/docs.

Preparing the Apache Servers to Deliver Extended Status

Add a section in the configuration file on each of the Apache servers for reading the extended status information of the server.

Follow these steps:

1. Open the **httpd.conf** file.

   This file is available at the following location:

   Windows Hosts: *C:\Program Files\Apache Software Foundation\Apache2.2\conf*

   Linux Hosts: *%PATH% /APACHE 2 / conf*

2. Activate the *LoadModule status_module modules/mod_status.so* in the file by removing the #-sign.

3. Add the following code snippet at the end of the file:

   ```
   ExtendedStatus On
   <Location /server-status>
   SetHandler server-status
   Order Deny,Allow
   Deny from all
   Allow from .nimsoft.no
   </Location>
   ```

   Note: Replace **.nimsoft.no** in the preceding example with your domain (or part of it). The *ExtendedStatus On* in the preceding example is optional and it is included only if you want to receive extended status. The extended status includes the detailed connection and request information of the server.

4. Restart the server after updating the configuration file for activating the new configuration settings.

   Use the command *din/apachectl –k restart* or use the apache service monitor for restarting the server.

Note: Select the **ExtendedStatus** on the probe GUI for each of the Apache servers.

Supported Platforms

Refer to the Nimsoft Compatibility Support Matrix for the latest information about supported platforms. See also the Support Matrix for Nimsoft Probes for more specific information about the Apache HTTP Server Monitoring probe.

Chapter 2: Configuration Details

You can configure the Apache HTTP Server Monitoring probe to monitor the status and performance of the apache web server. You can add the target apache web server to the Apache HTTP Server Monitoring probe and can configure the monitoring checkpoints. You can classify these servers under logical groups.

This section contains the following topics:

apache Node

The apache node is used to configure the general elements of the Apache HTTP Server Monitoring probe. These elements are applicable to all monitoring checkpoints of an apache web server.

Navigation: apache

Set or modify the following values that are based on your requirement:

apache > Probe Information

This section provides information about the probe name, probe version, start time of the probe, and the vendor who created the probe.

apache > General Configuration

This section allows you to configure the log properties and timeout settings for the Apache HTTP Server Monitoring probe.

- Log level: Specifies the level of details that are written to the log file.

  Default: 0 - Fatal

  Note: Recommendation is to select a lower log level during the normal operation and minimize the disk consumption. You can increase the log level while debugging.

- Total Operation Timeout (Seconds): Defines the time limit in seconds for completing a request between the Apache web server and the probe.

  Default: 300

- Connect Timeout (Seconds): Defines the time limit for establishing a connection between the Apache web server and the probe.

  Default: 10

apache > Message Pool

This section allows you to view default alarm messages for the different error conditions. The upper part of the section displays a list of messages. You can select a message row and the message attributes are displayed on the lower part of the section.

Profile-<Host Name> Node

The Profile-*host name* node is used to configure the host name or the IP address of the system, where the Apache HTTP server is hosted. This node is displayed as a child node under the *group name* node.

Note: This node is named as the Profile-*host name* throughout this document as the host name is user-configurable.

Navigation: apache > Profile-*host name*

Set or modify the following values that are based on your requirement:

Profile-*host name* > Apache Host Information

This section is used to update the host name or IP address of the Apache HTTP server.

Application Server Node

The **Application Server** node is used to configure host-specific properties and checkpoints, which the probe is monitoring. Each Apache host is displayed as a child node under the *host name* node.

Navigation: apache > Profile-*host name* > *host name* > Application Server

Set or modify the following values that are based on your requirement:

Application Server > Host Configuration

This section is used to configure the basic properties, which are necessary for the probe to connect and start a communication with the Apache host.

- Hostname or IP address: Defines the host name or IP address of the system, where the Apache web server is hosted.
- Alarm Message: Specifies the alarm message to be issued, when the Apache web server host does not respond.
- Override Default Suppression ID: Allows you to override the default suppression id with the specified suppression id.
- Suppression ID: Defines the new suppression id (overriding the default suppression ID) for filtering out certain alarm messages.
- Server Address for HTTP Response and Server Status: Defines the server address in the **<server address>/server-status?auto** format. For example, www.apache.org/server-status?auto.
- Data Collection Interval: Specifies the time interval for collecting data from the Apache web server.

  Default: 1 minute
- Extended Status: Allows you to collect extended status (including detailed connection and request information) from the Apache web server. This option works only if the Apache server configuration file is configured for providing the necessary details.

  Default: Not selected
- Use SSL: Enables or disables the SSL certificate verification.

  Default: Not selected
- Peer Verification: Enables or disables the peer verification. Peer is the certification authority who issues the SSL certificates.

  Default: Not selected
- Certification Authority Bundle Path: Specifies the certification bundle path for the SSL verification. The bundle contains certificates of all the issuing authorities. For the verification of SSL certificates, the certification bundle path is necessary.

- Host Verification: Enables or disables the host verification. This option verifies whether the hostname matches the names that are stored in the server certificate.

  Default: Not selected

- Host Verification Level: Specifies one of the following levels for verifying a host:
  - Loose: The host name is not verified against the CN (Common Name) attribute appearing in the SSL certificate. The verification checks if the IP address or host name points to the same server.
  - Strict: The host name is verified against the CN (Common Name) attribute appearing in the SSL certificate. If the host name does not match the CN field, the session request gets rejected.

Application Server > Agent Error

This section contains configuration details of the message agent alarm.

Apache Server Node

The **Apache Server** node (added by default for each host) is used to configure the checkpoints for the hosts being monitored. The checkpoints are configured for fulfilling the monitoring requirements. These checkpoints are classified under the following nodes:

- Connection
- Connection Mode
- ScoreBoard
- ScoreBoard %
- Server

Connection Node

The **Connection** node is used to configure the following checkpoints:

- **Child Avg Mbytes:** Average value of the child (megabytes transferred this child) for all current connections.
- **Child Max Mbytes:** Maximum value of the child (megabytes transferred this child) for any current connection.
- **Conn Avg Kbytes:** Average value of the connection (megabytes transferred this connection) for all current connections.
- **Conn Max Kbytes:** Maximum value of the connection (megabytes transferred this connection) for any current connection.
- **Request Avg Time:** Average value of the request (milliseconds required to process most recent request) from all current connections.

- **Request Max Time:** Maximum value of the request (milliseconds required to process most recent request) from any current connection.
- **Slot Avg Mbytes:** Average value of the slot (total megabytes transferred this slot) from all current connections.
- **Slot Max Mbytes:** Maximum value of the slot (total megabytes transferred this slot) from any current connection.
- **SS Avg Time:** Average value of SS (seconds from the beginning time of the most recent request) for all current connections.
- **SS Max Time:** Maximum value of SS (seconds from the beginning time of the most recent request) for any current connection.

Note: Each checkpoint is added as a separate section under the **Connection** node.

Navigation: apache > Profile-*host name* > *host name* > Application Server > Apache Server > Connection

Set or modify the following values that are based on your requirement:

Connection > Child Avg Mbytes

This section is used to configure the **Child Avg Mbytes** checkpoint.

- Active: Activates the monitoring of the checkpoint.

  Default: Not selected
- Name: Identifies the checkpoint name.
- Class: Identifies the checkpoint class, under which the checkpoint is classified.
- Group: Identifies the group name of the checkpoint. The group can either be Connection or Server.
- Monitoring Object: Identifies the Apache object, which is under monitoring by the checkpoint. This object is preconfigured against each checkpoint in the probe.
- Description: Identifies the description of the monitoring object.
- Compute Average: Allows you to calculate average of the values that are measured during the selected time interval and then compare it with the threshold value. Select one of the predefined intervals from the drop-down list.
- Operator: Specifies the threshold operator.
- Threshold Value: Defines the alarm threshold value. In case, this value is breached (see the Value and Operator fields) alarm is raised.
- Message Token: Specifies the alarm message, which is issued when the specified threshold value is breached. These messages are kept in the Message Pool.

- Override Default Suppression ID: Allows you to override the default suppression id with the specified suppression id.

  Default: Not selected

- Suppression ID: Defines the suppression id (overriding the default suppression ID) using which you want to filter out certain alarm messages.

Note: You can configure the other checkpoints same as the **Child Avg Mbytes** checkpoint.

Connection Mode Node

The **Connection Mode** node is used to configure the following checkpoints:

- **Mode-C SS Max Time:** The maximum occurrence of SS (Seconds from the beginning time of the most recent request) where Mode of the operation = C (The closing connection).
- **Mode-C SS Avg Time:** The current average of all SS where Mode = C.
- **Mode-D SS Max Time:** The maximum occurrence of SS (seconds from the beginning time of the most recent request) where Mode of the operation = D (The DNS lookup).
- **Mode-D SS Avg Time:** The current average of all SS where Mode = D.
- **Mode-K SS Max Time:** The maximum occurrence of SS (seconds from the beginning time of the most recent request) where Mode of the operation = K (Keepalive (read)).
- **Mode-K SS Avg Time:** The current average of all SS where Mode = K.
- **Mode-L SS Max Time:** The maximum occurrence of SS (seconds from the beginning time of the most recent request) where Mode of the operation = L (Logging).
- **Mode-L SS Avg Time:** The current average of all SS where Mode = L.
- **Mode-R SS Max Time:** The maximum occurrence of SS (seconds from the beginning time of the most recent request) where Mode of the operation = R (Reading Request).
- **Mode-R SS Avg Time:** The current average of all SS where Mode = R.
- **Mode-W SS Max Time:** The maximum occurrence of SS (seconds from the beginning time of the most recent request) where Mode of the operation = W (Sending Reply).

- **Mode-W SS Avg Time:** The current average of all SS where Mode = W.

Note: Each checkpoint is added as a separate section under the **Connection Mode** node.

Navigation: apache > Profile-*host name* > *host name* > Application Server > Apache Server > Connection Mode

Set or modify the following values that are based on your requirement:

Connection Mode > Mode-C SS Max Time

This section is used to configure the **Mode-C SS Max Time** checkpoint.

- Class: Identifies the checkpoint class, under which the checkpoint is classified.
- Group: Identifies the group name of the checkpoint. The group can either be Connection or Server.
- Monitoring Object: Identifies the Apache object, which is under monitoring by the checkpoint. This object is preconfigured against each checkpoint in the probe.
- Compute Average: Allows you to calculate average of the values that are measured during the selected time interval and then compare it with the threshold value. Select one of the predefined intervals from the drop-down list.
- Operator: Specifies the threshold operator.
- Threshold Value: Defines the alarm threshold value. In case, this value is breached (see the Value and Operator fields) alarm is raised.
- Message Token: Specifies the alarm message, which is issued when the specified threshold value is breached. These messages are kept in the Message Pool.
- Override Default Suppression ID: Allows you to override the default suppression id with the specified suppression id.

  Default: Not selected
- Suppression ID: Defines the suppression id (overriding the default suppression ID) using which you want to filter out certain alarm messages.

Note: You can configure the other checkpoints same as the **Mode-C SS Max Time** checkpoint.

ScoreBoard Node

The **ScoreBoard** node is used to configure the following checkpoints:

- **Closing Connection:** Number of workers currently closing a connection.
- **DNS Lookup:** Number of workers currently requesting the DNS lookup.
- **Gracefully Finishing:** Number of workers currently gracefully finishing connections.

- **Idle Cleanup Of Worker:** Number of workers, which are currently performing idle cleanup procedure.
- **Keepalive:** Number of workers currently sending keepalive messages.
- **Logging:** Number of workers currently busy updating log files.
- **Open Slot No Current Process:** Number of workers currently not busy with any process.
- **Reading Request:** Number of workers currently reading incoming requests.
- **Sending Reply:** Number of workers currently sending a reply.
- **Starting Up:** Number of workers currently starting up a connection.
- **Waiting For Connection:** Number of workers currently waiting for a connection.

Note: Each checkpoint is added as a separate section under the **ScoreBoard** node.

Navigation: apache > Profile-*host name* > *host name* > Application Server > Apache Server > ScoreBoard

Set or modify the following values that are based on your requirement:

ScoreBoard > Closing Connection

This section is used to configure the **Closing Connection** checkpoint.

- Class: Identifies the checkpoint class, under which the checkpoint is classified.
- Group: Identifies the group name of the checkpoint. The group can either be Connection or Server.
- Monitoring Object: Identifies the Apache object, which is under monitoring by the checkpoint. This object is preconfigured against each checkpoint in the probe.
- Compute Average: Allows you to calculate average of the values that are measured during the selected time interval and then compare it with the threshold value. Select one of the predefined intervals from the drop-down list.
- Operator: Specifies the threshold operator.
- Threshold Value: Defines the alarm threshold value. In case, this value is breached (see the Value and Operator fields) alarm is raised.
- Message Token: Specifies the alarm message, which is issued when the specified threshold value is breached. These messages are kept in the Message Pool.
- Override Default Suppression ID: Allows you to override the default suppression id with the specified suppression id.

  Default: Not selected

- Suppression ID: Defines the suppression id (overriding the default suppression ID) using which you want to filter out certain alarm messages.

Note: You can configure the other checkpoints same as the **Closing Connection** checkpoint.

ScoreBoard % Node

The **ScoreBoard %** node is used to configure the following checkpoints:

- **Closing Connection Pct:** Percentage of workers currently closing a connection.
- **DNS Lookup Pct:** Percentage of workers currently requesting the DNS lookup.
- **Gracefully Finishing Pct:** Percentage of workers currently gracefully finishing connections.
- **Idle Cleanup Of Worker Pct:** Percentage of workers currently performing idle cleanup procedure.
- **Keepalive Pct:** Percentage of workers currently sending keepalive messages.
- **Logging Pct:** Percentage of workers currently busy updating log files.
- **Open Slot No Current Process Pct:** Percentage of workers currently not busy with any process.
- **Reading Request Pct:** Percentage of workers currently reading incoming requests.
- **Sending Reply Pct:** Percentage of workers currently sending a reply.
- **Starting Up Pct:** Percentage of workers currently starting up a connection.
- **Waiting For Connection Pct:** Percentage of workers currently waiting for a connection.

Note: Each checkpoint is added as a separate section under the **ScoreBoard %** node.

Navigation: apache > Profile-*host name* > *host name* > Application Server > Apache Server > ScoreBoard %

Set or modify the following values that are based on your requirement:

ScoreBoard % > Closing Connection Pct

This section is used to configure the **Closing Connection Pct** checkpoint.

- Class: Identifies the checkpoint class, under which the checkpoint is classified.
- Group: Identifies the group name of the checkpoint. The group can either be Connection or Server.
- Monitoring Object: Identifies the Apache object, which is under monitoring by the checkpoint. This object is preconfigured against each checkpoint in the probe.

- Compute Average: Allows you to calculate average of the values that are measured during the selected time interval and then compare it with the threshold value. Select one of the predefined intervals from the drop-down list.
- Operator: Specifies the threshold operator.
- Threshold Value: Defines the alarm threshold value. In case, this value is breached (see the Value and Operator fields) alarm is raised.
- Message Token: Specifies the alarm message, which is issued when the specified threshold value is breached. These messages are kept in the Message Pool.
- Override Default Suppression ID: Allows you to override the default suppression id with the specified suppression id.

  Default: Not selected
- Suppression ID: Defines the suppression id (overriding the default suppression ID) using which you want to filter out certain alarm messages.

Note: You can configure the other checkpoints same as the **Closing Connection Pct** checkpoint.

Server Node

The **Server** node is used to configure the following checkpoints:

- **Busy Workers:** Number of active threads.
- **Bytes/req:** Number of bytes transferred per request.
- **CPU Load:** Current cpu load on server.

  Note: This checkpoint is not available on Windows servers.
- **Http Response Time:** Time for handling server-page request.
- **Http Response Value:** Is server responding?
- **Idle Workers:** Number of idle threads.
- **Request/S:** Number of requests per second.

Note: Each checkpoint is added as a separate section under the **Server** node.

Navigation: apache > Profile-*host name* > *host name* > Application Server > Apache Server > Server

Set or modify the following values that are based on your requirement:

Server > Busy Workers

This section is used to configure the **Busy Workers** checkpoint.

- Class: Identifies the checkpoint class, under which the checkpoint is classified.

- Group: Identifies the group name of the checkpoint. The group can either be Connection or Server.
- Monitoring Object: Identifies the Apache object, which is under monitoring by the checkpoint. This object is preconfigured against each checkpoint in the probe.
- Compute Average: Allows you to calculate average of the values that are measured during the selected time interval and then compare it with the threshold value. Select one of the predefined intervals from the drop-down list.
- Operator: Specifies the threshold operator.
- Threshold Value: Defines the alarm threshold value. In case, this value is breached (see the Value and Operator fields) alarm is raised.
- Message Token: Specifies the alarm message, which is issued when the specified threshold value is breached. These messages are kept in the Message Pool.
- Override Default Suppression ID: Allows you to override the default suppression id with the specified suppression id.

  Default: Not selected
- Suppression ID: Defines the suppression id (overriding the default suppression ID) using which you want to filter out certain alarm messages.

Note: You can configure the other checkpoints same as the **Busy Workers** checkpoint.

Configure a Node

This procedure provides the information to configure a particular section within a node.

Each section within the node allows you to configure the properties of the probe for monitoring the Apache web server.

Follow these steps:

1. Select the appropriate navigation path.
2. Update the field information and click **Save**.

   The specified section of the probe is configured. The probe is now ready to monitor your Apache web server.

Configure Dynamic Alarm Thresholds

Dynamic thresholds are configured at the QoS metric level in each probe that publishes an alarm for a QoS metric.

Important! In order to create dynamic alarm thresholds, you must have the baseline_engine probe version 2.0 installed on the robot and configured.

Follow these steps for each QoS metric where you want to configure dynamic thresholds:

1. Select a node in the tree to view any associated monitors and QoS metrics.
2. Select the monitor you want to modify in the table.
3. Select the Publish Data and Compute Baseline options to enable the Dynamic Alarm Thresholds section of the configuration.
4. Choose a threshold algorithm. There are three algorithms allowed for dynamic alarm thresholds:

   Note: You must indicate the direction for each algorithm, either increasing or decreasing.

   - Scalar: Each threshold is a specific value from the computed baseline.
   - Percent: Each threshold is a specific percentage of the computed baseline.
   - Standard Deviation: Each threshold is a measure of the variation from the computed baseline. A large standard deviation indicates that the data points are far from the computed baseline and a small standard deviation indicates that they are clustered closely around the computed baseline.

   Important! To change the subsystem ID, you must have the baseline_engine probe version 2.1 installed on the robot and configured.
5. (Optional) If the Subsystem ID listed in the Subsystem (default) field is not correct for your configuration, enter the correct ID in the Subsystem (override) field.
6. Save your settings.

Add Host

The apache host server is required to be added to the Apache HTTP Server Monitoring probe start monitoring. The probe can connect and request necessary information from the apache server, after adding the host.

Follow these steps:

1. Click the **Options** icon next to the *group name* node in the navigation pane.
2. Click the **Add New Host** option.

3. Enter the information in the **New Host Configuration** dialog and click **Submit**.

   The host is added as a child node under the selected *group name* node.

Note: A host named **localhost** is added, by default, to the probe.

Delete Host

You can delete a host that is no longer required monitoring.

Follow these steps:

1. Click the **Options** icon next to the *host name* node in the navigation pane.
2. Click the **Delete Host** option.
3. Click **Save**.

   The selected *host name* node is removed from the navigation pane.

Chapter 3: QoS Threshold Metrics

Many CA Nimsoft Monitor probes ships with the default QoS threshold values set. The default threshold values provide an idea of the type of values to be entered in the fields. These default values are not necessarily recommended best practice values. To aid in tuning thresholds and reducing false-positive alarms, this section describes the QoS metrics and provides the default QoS thresholds.

This section contains the following topics:

apache QoS Metrics

The following table describes the checkpoint metrics that can be configured using the Apache HTTP Server Monitoring probe.

Metric Name	Units	Description
QOS_APACHE_BUSYWORKERS		Busy workers
QOS_APACHE_BYTESPERREQ	Byte	Bytes per request
QOS_APACHE_CHLDAVEMBYTES	MBytes	Child Ave mbytes
QOS_APACHE_CLOSINGCONNECTIONPCT	Percent	Connection closing percent
QOS_APACHE_CONNAVEKBYTES	KBytes	Connection Ave kbytes
QOS_APACHE_CPULOAD	Percent	CPU load
QOS_APACHE_HTTPRESTIME	Milliseconds	http response time
QOS_APACHE_IDLEWORKERS		Idle workers
QOS_APACHE_KEEPALIVE		Connection keepalive
QOS_APACHE_OPENSLOTNOCURRENTREQUESTPCT	Percent	Connection Open slot no current request percent
QOS_APACHE_READINGREQUEST		Connection reading request
QOS_APACHE_REQMAXTIME	Millisecond	Request Max time

Metric Name	Units	Description
QOS_APACHE_REQPERSEC		Request per second
QOS_APACHE_SENDINGREPLY		Connection sending reply
QOS_APACHE_SLOTAVEMBYTES	MBytes	Slot Ave Mbytes
QOS_APACHE_SSAVETIME	Seconds	SS Ave time
QOS_APACHE_SSMAXTIME	Seconds	SS Max time
QOS_APACHE_STATECSSAVETIME	Seconds	Mode C SS Ave time
QOS_APACHE_STATEDSSAVETIME	Seconds	Mode D SS Ave time
QOS_APACHE_STATEKSSAVETIME	Seconds	Mode K SS Ave time
QOS_APACHE_STATELSSAVETIME	Seconds	Mode L SS Ave time
QOS_APACHE_STATERSSAVETIME	Seconds	Mode R SS Ave time
QOS_APACHE_STATEWSSAVETIME	Seconds	Mode W SS Ave time
QOS_APACHE_WAITINGFORCONNECTIONPCT	Percent	Connection waiting for connection percent

apache Alert Metrics Default Settings

This table contains the alert metrics default settings for the Apache HTTP Server Monitoring probe.

QoS Metric	Warning Threshold	Warning Severity	Error Threshold	Error Severity	Description
MsgAgentError	-	-	-	Critical	If the server is not running on $host, MsgAgentError will come.
MsgWarning	-	-	-	Warning	If the Checkpoint breaches threshold, MsgWarning will come.

QoS Metric	Warning Threshold	Warning Severity	Error Threshold	Error Severity	Description
MsgError	-	-	-	Critical	If the Checkpoint breaches threshold, MsgError will come.