CA Application Performance Management

for Web Servers Guide

Release 9.1.1



This Documentation, which includes embedded help systems and electronically distributed materials, (hereinafter referred to as the “Documentation”) is for your informational purposes only and is subject to change or withdrawal by CA at any time.

This Documentation may not be copied, transferred, reproduced, disclosed, modified or duplicated, in whole or in part, without the prior written consent of CA. This Documentation is confidential and proprietary information of CA and may not be disclosed by you or used for any purpose other than as may be permitted in (i) a separate agreement between you and CA governing your use of the CA software to which the Documentation relates; or (ii) a separate confidentiality agreement between you and CA.

Notwithstanding the foregoing, if you are a licensed user of the software product(s) addressed in the Documentation, you may print or otherwise make available a reasonable number of copies of the Documentation for internal use by you and your employees in connection with that software, provided that all CA copyright notices and legends are affixed to each reproduced copy.

The right to print or otherwise make available copies of the Documentation is limited to the period during which the applicable license for such software remains in full force and effect. Should the license terminate for any reason, it is your responsibility to certify in writing to CA that all copies and partial copies of the Documentation have been returned to CA or destroyed.

TO THE EXTENT PERMITTED BY APPLICABLE LAW, CA PROVIDES THIS DOCUMENTATION “AS IS” WITHOUT WARRANTY OF ANY KIND, INCLUDING WITHOUT LIMITATION, ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NONINFRINGEMENT. IN NO EVENT WILL CA BE LIABLE TO YOU OR ANY THIRD PARTY FOR ANY LOSS OR DAMAGE, DIRECT OR INDIRECT, FROM THE USE OF THIS DOCUMENTATION, INCLUDING WITHOUT LIMITATION, LOST PROFITS, LOST INVESTMENT, BUSINESS INTERRUPTION, GOODWILL, OR LOST DATA, EVEN IF CA IS EXPRESSLY ADVISED IN ADVANCE OF THE POSSIBILITY OF SUCH LOSS OR DAMAGE.

The use of any software product referenced in the Documentation is governed by the applicable license agreement and such license agreement is not modified in any way by the terms of this notice.

The manufacturer of this Documentation is CA.

Provided with “Restricted Rights.” Use, duplication or disclosure by the United States Government is subject to the restrictions set forth in FAR Sections 12.212, 52.227-14, and 52.227-19(c)(1) - (2) and DFARS Section 252.227-7014(b)(3), as applicable, or their successors.

Copyright © 2012 CA. All rights reserved. All trademarks, trade names, service marks, and logos referenced herein belong to their respective companies.

CA Technologies Product References

This document references the following CA Technologies products and features:

- CA Application Performance Management (CA APM)
- CA Application Performance Management ChangeDetector (CA APM ChangeDetector)
- CA Application Performance Management ErrorDetector (CA APM ErrorDetector)
- CA Application Performance Management for CA Database Performance (CA APM for CA Database Performance)
- CA Application Performance Management for CA SiteMinder (CA APM for CA SiteMinder)
- CA Application Performance Management for CA SiteMinder Application Server Agents (CA APM for CA SiteMinder Application Server Agents)
- CA Application Performance Management for CA SYSVIEW® (CA APM for CA SYSVIEW)
- CA Application Performance Management for IBM CICS Transaction Gateway (CA APM for IBM CICS Transaction Gateway)
- CA Application Performance Management for IBM WebSphere Application Server (CA APM for IBM WebSphere Application Server)
- CA Application Performance Management for IBM WebSphere Distributed Environments (CA APM for IBM WebSphere Distributed Environments)
- CA Application Performance Management for IBM WebSphere MQ (CA APM for IBM WebSphere MQ)
- CA Application Performance Management for IBM WebSphere Portal (CA APM for IBM WebSphere Portal)
- CA Application Performance Management for IBM WebSphere Process Server (CA APM for IBM WebSphere Process Server)
- CA Application Performance Management for IBM z/OS® (CA APM for IBM z/OS)
- CA Application Performance Management for Microsoft SharePoint (CA APM for Microsoft SharePoint)
- CA Application Performance Management for Oracle Databases (CA APM for Oracle Databases)
- CA Application Performance Management for Oracle Service Bus (CA APM for Oracle Service Bus)
- CA Application Performance Management for Oracle WebLogic Portal (CA APM for Oracle WebLogic Portal)

- CA Application Performance Management for Oracle WebLogic Server (CA APM for Oracle WebLogic Server)
- CA Application Performance Management for SOA (CA APM for SOA)
- CA Application Performance Management for TIBCO BusinessWorks (CA APM for TIBCO BusinessWorks)
- CA Application Performance Management for TIBCO Enterprise Message Service (CA APM for TIBCO Enterprise Message Service)
- CA Application Performance Management for Web Servers (CA APM for Web Servers)
- CA Application Performance Management for webMethods Broker (CA APM for webMethods Broker)
- CA Application Performance Management for webMethods Integration Server (CA APM for webMethods Integration Server)
- CA Application Performance Management Integration for CA CMDB (CA APM Integration for CA CMDB)
- CA Application Performance Management Integration for CA NSM (CA APM Integration for CA NSM)
- CA Application Performance Management LeakHunter (CA APM LeakHunter)
- CA Application Performance Management Transaction Generator (CA APM TG)
- CA Customer Experience Manager (CA CEM)
- CA Embedded Entitlements Manager (CA EEM)
- CA eHealth® Performance Manager (CA eHealth)
- CA Insight™ Database Performance Monitor for DB2 for z/OS
- CA Introscope® (CA Introscope (R))
- CA SiteMinder®
- CA Spectrum® Infrastructure Manager (CA Spectrum)
- CA SYSVIEW® Performance Management (CA SYSVIEW)

Contact CA Technologies

Contact CA Support

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

- 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

If you have comments or questions about CA Technologies product documentation, you can send a message to techpubs@ca.com.

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

Documentation Changes

The following changes have been made since the last release of this documentation:

- Rebranding with the new CA APM for Web Servers product name.
- Enhanced product documentation to reflect minor fixes toD CA APM for Web Servers.

Product Documentation

CA APM documentation includes information for CA APM, CA Introscope (R), CA CEM, and CA APM extensions and integrations.

You can view and search all the titles in the CA APM documentation set from the CA APM bookshelf on the CA Support Online (CSO) website.

The following list shows the documentation specific to CA APM.

- *CA APM Release Notes* — Release summary information for CA APM.

  Note: In previous releases, this document was titled *CA APM ReadMe.*

- *CA APM Readme* — Important last-minute release information for CA APM; available on the CA APM software download site or CA Support site.

  Note: In previous releases, this document was titled *CA APM Known Issues.*

- *CA APM Installation and Upgrade Guide* — Installation requirements; installing CA APM, including installing CA Introscope (R), Enterprise Manager, APM database, Workstation, WebView, CA CEM, TIM; upgrading from previous releases.
- *CA APM Overview Guide* — A broad overview of CA APM components and architecture. Explains terms and concepts used in a CA APM deployment.
- *CA APM Configuration and Administration Guide* — Combines configuration and administration information for CA Introscope (R) and for CA CEM. CA Introscope (R) and CA CEM properties are documented in the appendix.
- *CA APM Security Guide* — Choosing and configuring CA APM, CA Introscope (R), and CA CEM security solutions. Includes information about Embedded Entitlements Manager.
- *CA APM Sizing and Performance Guide* — Sizing, tuning, and capacity planning for your CA APM deployment and components.
- *CA APM Transaction Definition Guide* — Transaction definition processes and procedures for CA APM; describes the necessary steps to record, define, and verify customer transactions.

The following list shows the documentation specific to CA Introscope (R). CA APM documentation is also pertinent for CA Introscope (R).

- *CA APM Java Agent Implementation Guide* — Installation, configuration, and use of the CA APM Java Agent.
- *CA APM .NET Agent Implementation Guide* — Installation, configuration, and use of the CA APM .NET Agent.

- *CA APM Environment Performance Agent Implementation Guide* — Implementing Environment Performance Agent (EPAgent) with CA Introscope (R) to monitor system information, including process availability, disk statistics, web application server and web server logs, Solaris KStat and HTTP service availability. The guide provides instructions for installing, configuring, and using EPAgent.
- *CA APM Workstation User Guide* — Using CA Introscope (R) dashboards, Investigator tree and application triage map, Transaction Tracer, and reporting. Includes CA Introscope (R) metrics overview and descriptions.
- *CA APM WebView User Guide* — Using WebView to view CA Introscope (R) data in dashboards and the Investigator.
- *CA APM ChangeDetector User Guide* — Using CA APM ChangeDetector to monitor and report changes in application files and configuration.
- *CA APM Transaction Generator Implementation Guide* — Using the CA APM Transaction Generator (CA APM TG) to monitor the availability, health, and performance of web sites and web services from the perspective of a user attempting to access web sites. How to use the CA APM TG Agent to generate synthetic transactions that you can monitor using CA APM.

The following list shows the documentation specific to extensions and integrations.

- *CA APM API Reference Guide* — Contains data and components managed within CA APM that is exposed to consumers with an application programming interface (API).
- *CA APM Catalyst Connector Guide* — Installing and using the Catalyst Connector for CA APM.
- *CA APM for CA SiteMinder SNMP Collector Guide* — Installing and configuring CA APM for CA SiteMinder SNMP Collector. Understanding the associated metrics.
- *CA APM for CA SiteMinder Applications Server Agents Guide* — Installing, configuring, and using CA APM for CA SiteMinder Applications Server Agents.
- *CA APM for IBM CICS Transaction Gateway Guide* — Installing, configuring, and using CA APM for IBM CICS Transaction Gateway.
- *CA APM for IBM WebSphere Application Server for Distributed Environments Guide* — Installing, configuring, and using CA APM for IBM WebSphere Distributed Environments.
- *CA APM for IBM WebSphere Application Server for z/OS Guide* — Installing, configuring, and using CA APM for IBM WebSphere for z/OS.
- *CA APM for IBM WebSphere MQ Guide* — Using CA Introscope (R) to view metrics from IBM WebSphere MQ.
- *CA APM for IBM WebSphere Portal Guide* — Installing, configuring, and using CA APM for IBM WebSphere Portal.
- *CA APM for IBM z/OS Guide* — Installing, configuring, and using CA APM for IBM z/OS.

- *CA APM for Microsoft SharePoint Guide* — Installing and configuring CA APM for Microsoft SharePoint to monitor your SharePoint components during development, QA, staging, and production.
- *CA APM for Oracle Databases Guide* — Installing, configuring, and using CA APM for Oracle Databases.
- *CA APM for Oracle WebLogic Portal Guide* — Installing, configuring, and using CA APM for Oracle WebLogic Portal.
- *CA APM for Oracle WebLogic Server Guide* — Installing, configuring, and using CA APM for Oracle WebLogic Server.
- *CA APM for SOA Implementation Guide* — Installation and configuration information for using CA APM for SOA and SOA platform extensions with CA Introscope (R).
- *CA APM for Web Servers Guide* — Installing, configuring, and using CA APM for Web Servers.
- *CA APM Integration for CA CMDB Guide* — Installing, configuring, and using CA APM for CA CMDB.
- *CA APM Integration for CA Infrastructure Management Guide* — Installing, configuring, and using CA APM for CA Infrastructure Management.
- *CA APM Integration for CA NSM Guide* — Installing, configuring, and using CA APM for CA NSM.
- *CA Cross-Enterprise Application Performance Management Integration Guide* — Installing, configuring, and using the SYSVIEW Agent extension, which allows you to manage application performance of distributed applications accessing mainframe back ends and trace transactions from distributed applications to mainframe CICS transactions. Allows you to monitor the health metrics of critical mainframe components.
- *CA Introscope (R) SAP NetWeaver Conversion Guide* — Using CA APM for SAP NetWeaver.
- *CA Introscope (R) WebView User Guide for SAP* — This guide is for SAP WebView users.

Note: In some product documentation, screenshots contain a logo or other reference to ‘Wily’, which CA Technologies has replaced with ‘APM.’ Ignore ‘Wily’ logos, as they have been removed in the current APM Workstation. References to ‘Wily’ in diagrams refer to CA Introscope (R).

Understanding Directory and File Name Conventions

This guide uses the following conventions in file names and directory paths:

Convention	Refers to
<Agent_Home>	The top-level directory where the CA Introscope (R) agent is installed. This directory is typically named *wily*.
<APM_Db_Home>	The top-level directory where the APM database is installed, when referring to Database-only installations.
<AppServer_Home>	The top-level directory where your application server is installed. This directory is often the same as *<Agent_Home>*.
<EM_Home>	The top-level directory where the Enterprise Manager is installed.
<ProductName_Home>	The installation directory of a third-party product or type of application. For example, it is the installation directory of the application server if you are using WebLogic.
<version>	Version-specific identifier included in file names or displayed in the user interface. For example, the following file name: com.wily.introscope.soa.dependencymap_<version>.jar represents a version-specific file name, such as: com.wily.introscope.soa.dependencymap_9.1.0.jar
<File_Name><VersionNumber><Operating System or other identifier>.FileType	A file name that includes specific identifying information. For example, if you extract files from a tar package for CA APM ChangeDetector 9.1.0.0 on a UNIX operating system, then download this file: ChangeDetector9.1.0.0unix.tar But, view it in this guide as follows: ChangeDetector<*VersionNumber*>.unix.tar

Convention	Refers to
Forward slash (/) path separators	The path separator used in directory names on your operating environment. The forward slash (/) is used on UNIX platforms and in examples throughout this guide, but use the separator appropriate for your operating system.
Dollar sign ($) environment variables	The environment variable notation used on your operating system. The dollar sign ($) is used in UNIX environments and in examples throughout this guide, but you use the character appropriate to your environment.

Contents

Chapter 1: Overview 17

CA APM for Web Servers Overview 17
CA APM for Web Servers Usage Scenarios 18
CA APM for Web Servers Functionality 18
Metrics 19

Chapter 2: Installing and configuring the CA APM for Web Servers 21

Prepare for Installing CA APM for Web Servers 21
View the Product Compatibility Guide 22
Installing CA APM for Web Servers components on Windows 23
Step 1: Running the Enterprise Manager installer on Windows 23
Step 2: Installing CA APM for Web Servers agent components on Windows 24
Step 3: Registering the CA APM for Web Servers as a Windows service 27
Step 4: Configuring the AgentConfig.properties file on Windows 27
Step 5: Configuring web servers to publish statistics 28
Step 6: Defining web servers to monitor 31
Step 7: Enabling the Management Module and dashboards 36
Step 8: (Optional) Customizing ApacheCustomMetrics.xml file 37
Step 9: Starting the CA APM for Web Servers on Windows 37
Step 10: Stopping the CA APM for Web Servers on Windows 38
Step 11: Unregistering the CA APM for Web Servers as a Windows service 38
Installing CA APM for Web Servers components on UNIX 39
Step 1: Running the Enterprise Manager installer on UNIX 39
Step 2: Installing CA APM for Web Servers agent components on UNIX 40
Step 3: Configuring the AgentConfig.properties file on UNIX 41
Step 4: Configuring web servers to publish statistics 42
Step 5: Defining web servers to monitor 43
Step 6: Enabling the Management Module and dashboards 43
Step 7: (Optional) Customizing ApacheCustomMetrics.xml file 43
Step 8: Starting the CA APM for Web Servers on UNIX 43
Step 9: Stopping the CA APM for Web Servers on UNIX 44
Step 10: (Optional) Restarting the CA APM for Web Servers or finding its status on UNIX 44
Upgrading the CA APM for Web Servers 45
Upgrading from an earlier version 46

Chapter 3: Using the CA APM for Web Servers 49

HTTPS support 49
Improved support for web servers 51
Changing Per Second Metrics to Per Interval 55
Configurable statistics page location 56

Chapter 4: Viewing data from the CA APM for Web Servers 57

Using the CA APM for Web Servers with Introscope Workstation 57
Viewing web server metrics in the Introscope Investigator tree 58
Viewing the CA APM for Web Servers dashboards 60
    Web Servers Availability dashboard 61
    Apache dashboards 62
    Sun ONE (iPlanet) dashboard 63
    Microsoft IIS Web Server dashboard 64

Appendix A: Metrics 65

CA APM for Web Servers metrics 65
Common metrics to all web servers 65
    Discovered Servers metrics 65
    Availability metrics 66
    Info metrics 66
Apache, IBM HTTP Server, and Oracle HTTP Server metrics 66
    Apache-based performance metrics 67
Microsoft Internet Information Services (IIS) metrics 69
    IIS performance metrics 69
iPlanet (Sun ONE) Web Server metrics 75
    iPlanet performance metrics 75

Appendix B: CipherSuites supported by CA APM for Web Servers 79

CA APM for Web ServersCipherSuites 79

Appendix C: Sizing recommendations 81

Metric Limits 81
Heap Sizing 83

Appendix D: Frequently Asked Questions 85

Upgrading the CA APM for Web Servers 85
Monitoring web servers 85

Discovery of web servers 88
Improved web server support 89
AgentConfigTool utility 90
General 91

Appendix E: IPv6 support 93

Connecting to Enterprise Manager on IPv6 93

Index 95

Chapter 1: Overview

This section describes the CA APM for Web Servers and how it fits into your CA Introscope deployment.

This section contains the following topics:

CA APM for Web Servers Overview (see page 17)
CA APM for Web Servers Functionality (see page 18)

CA APM for Web Servers Overview

CA APM for Web Servers enables you to monitor the availability and performance of popular web servers, such as Apache, Microsoft Internet Information Services (IIS), IBM HTTP Server, Oracle HTTP Server, and Sun ONE Web Server. With this extension, web server administrators can quickly detect and resolve web server availability and performance problems.

To help web server administrators find and fix problems, the CA APM for Web Servers provides the following:

- Alerts that indicate the availability for each web server.
- Performance statistics that track the web server load, throughput, cache usage, and the number of threads or processes idle or in use.
- Details about the time spent on various tasks for each web server.
- Predefined dashboards to enable quick diagnosis of the most common web server issues.

The CA APM for Web Servers provides the following capabilities:

Minimal setup

- Auto-discovery finds all web servers on your network
- Auto-configuration tunes CA APM for Web Servers settings as required for each individual type of web server
- Agentless design means there's nothing to install on each web server.

Dynamic reconfiguration

- Auto-discovery detects changes to web server and adjust its monitoring settings accordingly, without any user intervention.

Improved Web Server support

- Supports customized and new versions of Apache web server, Apache-based web servers, and new releases of Microsoft IIS and Sun ONE.

CA APM for Web Servers Usage Scenarios

Web server administrators can use the powerpack to diagnose the following issues:

- **Web server availability:** When users report that certain web applications are unavailable, the powerpack reports availability of all web servers, enabling administrators to rapidly determine if the web servers are actually unavailable.
- **Slow response times:** When users report slow page download times, the powerpack shows which servers are experiencing the highest load and have the highest response time.
- **Domain Name System (DNS) issues:** When web server administrators want to check whether DNS issues are due to application performance, the powerpack shows which web servers are spending excessive time on DNS lookups.
- **Load balancing issues:** When web server administrators want to check whether load balancer issues are slowing performance, the powerpack shows the relative amount of load for each web server and highlights over-loaded and under-loaded web servers.
- **Web server configuration issues:** When administrators want to check whether web server configuration issues are slowing performance, the powerpack highlights configuration issues related to worker processes or threads, cache misses, and so on.

CA APM for Web Servers Functionality

You can install the CA APM for Web Servers on any machine behind a firewall. You configure the monitored web server(s) to publish the performance statistics to a URL on that web server. The CA APM for Web Servers periodically connects remotely via HTTP or HTTPS to the web server, collects the statistics, and reports it to Introscope. You can configure the CA APM for Web Servers to automatically discover and monitor any new web server or web servers that appear on the specified subnet or subnets.

Metrics

The CA APM for Web Servers provides metrics specific to many popular web servers.

- Availability—whether a web server is available or not.
- Apache and IIS Worker Status—the number of busy or idle worker threads, idle pool threads, logging, DNS lookup, and so on.
- Response Time—amount of time used by the web server to process a request.
- Sun ONE—cache, connection queue, keep alive, native thread pools, and session creation.
- Microsoft IIS—asynchronous I/O, caching, connections, errors, I/O, requests, and user data.

Chapter 2: Installing and configuring the CA APM for Web Servers

This section describes how to install and configure the CA APM for Web Servers in an Introscope deployment.

This section contains the following topics:

Prepare for Installing CA APM for Web Servers (see page 21)
Installing CA APM for Web Servers components on Windows (see page 23)
Installing CA APM for Web Servers components on UNIX (see page 39)
Upgrading the CA APM for Web Servers (see page 45)

Prepare for Installing CA APM for Web Servers

Because the CA APM for Web Servers is an add-on feature for Introscope, verify information about your environment before you install. Reviewing your environment and preparing for installation helps ensure that you can install and configure the CA APM for Web Servers quickly and efficiently.

Follow these steps:

1. Review the system requirements.

   Note: For system requirements, see the *Compatibility Guide*.

2. Verify that you have the following components:

   - One or more supported web servers that you want to monitor installed and running.
   - At least one Enterprise Manager is installed and running.
   - At least one Introscope Workstation that can connect to the Enterprise Manager.

   Note: For more information about installing Introscope components, see the *CA APM Installation and Upgrade Guide*.

3. Identify the following directory locations in your Introscope environment:

   - The Enterprise Manager installation directory. This directory location is referred to as *<IntroscopeHome>*.
   - The installation directory that you want to use for the CA APM for Web Servers. You specify the path to this directory during installation. This directory location is referred to as *<PPWebServersHome>*.

4. Verify that you have the host name and port number for the Enterprise Manager to which the web servers will report data.
5. Verify that you have Sun JRE 1.5 at a minimum available on the computer where you plan to install the CA APM for Web Servers agent.
6. Update the PATH user variable to point to this JRE identified in the previous step.

   To update the PATH on Windows:
   `PATH=%JAVA_HOME%\bin;%PATH%`

   To update the PATH on UNIX:
   `export PATH=$JAVA_HOME/bin:$PATH`

   Important! You can use the CA APM for Web Servers on 64-bit platforms when you have the Sun JRE 1.5 or later 32-bit version.

More information:

View the Product Compatibility Guide (see page 22)

View the Product Compatibility Guide

The product Compatibility Guide provides a list of all supported operating environments.

Follow these steps:

1. Open a browser and go to http://www.ca.com/support.

   The CA Support Online page appears.
2. Log in to CA Support Online.
3. Select CA Application Performance Management from the Support By Product, Select a Product page drop-down list.

   The CA Application Performance Management page appears.
4. Scroll to the Product Status section and click the Application Performance Management Compatibility Guide link.

   The Application Performance Management Compatibility Guide page appears.
5. Click the link that corresponds to the release you want.

   The Compatibility Matrix appears.

Installing CA APM for Web Servers components on Windows

Installing and configuring the CA APM for Web Servers on Windows involves the following steps:

Step 1: Running the main Enterprise Manager installer on Windows (see page 23)

Step 2: Installing CA APM for Web Servers agent components on Windows (see page 27)

Step 3: Registering the CA APM for Web Servers as a Windows service (see page 27)

Step 4: Configuring the AgentConfig.properties file on Windows (see page 27)

Step 5: Configuring web servers to publish statistics (see page 28)

Step 6: Defining web servers to monitor (see page 31)

Step 7: Enabling the Management Module and dashboards (see page 36)

Step 8: (Optional) Customizing ApacheCustomMetrics.xml file (see page 37)

Step 9: Starting the CA APM for Web Servers on Windows (see page 37)

Step 10: Stopping the CA APM for Web Servers on Windows (see page 38)

Step 11: Unregistering the CA APM for Web Servers as a Windows service (see page 38)

The following sections describe these steps in detail.

Step 1: Running the Enterprise Manager installer on Windows

Run the Enterprise Manager installer to install the CA APM for Web Servers along with the Enterprise Manager.

Note: If you are using an Enterprise Manager that is already being used by a different agent, then the Enterprise Manager components of all the CA APM for Web Servers are already installed in the *<IntroscopeHome>/examples* directory. You do not have to continue with this step and instead can continue with configuring the Enterprise Manager.

The Enterprise Manager installer places the files into the *<IntroscopeHome>\examples\PowerPackForWebServers* directory. You will later move the files to the correct location, based on how they are organized in the *\examples* directory.

For details about the Enterprise Manager installer and where to find the Enterprise Manager installer executable, see the *CA APM Installation and Upgrade Guide*.

The Enterprise Manager installer places the following files onto the Enterprise Manager machine:
<IntroscopeHome>\examples\PowerPackForWebServers\config\modules\PPWebServers_ManagementModule.jar

This file is the CA APM for Web Servers Management Module, which contains pre-configured dashboards.

Step 2: Installing CA APM for Web Servers agent components on Windows

Run the Standalone agent installer to install and configure the CA APM for Web Servers agent information. This installer configures the agent with the Enterprise Manager host and port number.

Although the CA APM for Web Servers does not install an agent on the web server to collect web server data, it uses agents to report the data back to the Enterprise Manager.

The Standalone agent installer configures the *config\WebServerAgent.profile* file with the following properties, based on your entries in the installer:

introscope.agent.enterprisemanager.transport.tcp.host.DEFAULT

The host setting must be either the host name or IP address of a machine with an Enterprise Manager on it.

introscope.agent.enterprisemanager.transport.tcp.port.DEFAULT

The value must be the port on which the Enterprise Manager listens for agent connections.

Default setting is 5001.

The port specified in this setting must match the port defined in the setting *introscope.enterprisemanager.port.agentlistener* in the *introscopeEnterpriseManager.properties* file for each matching Enterprise Manager.

You can also define the properties that control the way agent connects to the Enterprise Manager, agent side metric aging, and metric clamping in the *WebServerAgent.profile* file. For more information about configuring agent properties, see the *CA APM Java Agent Implementation Guide* or the *CA APM .NET Agent Implementation Guide*.

For more information about running the Standalone agent installer, see the *CA APM Installation and Upgrade Guide*.

The CA APM for Web Servers agent files on Windows

The Standalone agent installer places the following files on the agent machine in the *<PPWebServersHome>* directory:

AgentConfigTool.bat

Batch file that configures the global and truststore settings for agent.

DeregisterWSService.bat

Batch file to unregister the CA APM for Web Servers as a Windows Service.

RegisterWSService.bat

Batch file to register the CA APM for Web Servers as a Windows Service.

ServerVersionFinder.bat

Batch file to find server header of a given HTTP or HTTPS web server URL.

UpdateMonitorConfigFile.bat

Batch file to upgrade the old WebServerConfig.xml to the new format.

.\config\AgentConfig.properties

Properties for CA APM for Web Servers agent. Use the AgentConfigTool.bat file to set these properties.

.\config\ApacheCustomMetrics.xml

Customizable file to map customized metric list to standard metric list. This is applicable to only Apache web server and web servers based on Apache.

.\config\DiscoveryConfig.xml

Configuration file to specify which subnets to scan for web servers.

.\config\WebServerAgent.profile

Profile for web server agent.

.\config\WebServerConfig.xml

Configuration file to specify which web servers to monitor.

.\lib\commons-logging-1.1.jar

A dependent JAR file for CA APM for Web Servers agent.

.\lib\jline-0.9.9.jar

JAR file used to mask the truststore password.

.\lib\PPWebServers.jar

CA APM for Web Servers JAR file.

.\lib\WebServerAgent.jar

Introscope web server agent; communicates web server statistics to Enterprise Manager.

.\lib\commons-codec-1.3.jar

A dependent JAR file for CA APM for Web Servers agent.

.\lib\ext\Supportability-Agent.jar

Introscope agent extension used for debugging by CA Support.

.\jsw-3.2.3*

This folder contains the Java Service Wrapper files used for registering CA APM for Web Servers agent as a Windows Service. You should modify only the .\jsw-3.2.3\conf\wrapper.conf file. It is recommended that you do not modify any other file in this folder.

If you select the CA APM for Web Servers IIS check box during the install, these files are extracted:

.\IIS\DeregisterVBScriptService.bat

Batch file to unregister the VB script as a Windows Service.

.\IIS\PublishIISStats.vbs

Script to collect statistics from IIS web servers.

.\IIS\RegisterVBScriptService.bat

Batch file to register the VB script as a Windows Service.

.\IIS\VBScript.bat

Batch file to launch PublishIISStats.vbs and publish IIS Metrics to the statistics page.

.\IIS\WinService.exe

Executable to register the VB Script as a service in the service control manager, if monitoring an IIS web server. This file needs to be copied to the machine where IIS is installed.

Step 3: Registering the CA APM for Web Servers as a Windows service

- Double Click the *RegisterWSService.bat* file to register the CA APM for Web Servers as a Windows service.

If you are running the CA APM for Web Servers on IIS web server, you should also run *RegisterVBScriptService.bat* on the IIS web server machine.

Note: CA APM for Web Servers does not start automatically. You need to manually start it.

More information:

Step 9: Starting the CA APM for Web Servers on Windows (see page 37)

Step 4: Configuring the AgentConfig.properties file on Windows

You can specify the global settings for the CA APM for Web Servers in the *AgentConfig.properties* file.

Important! If your web server functions in permissive mode, you do not have set trustore properties.

This file has the following properties:

- the path to the Web Server Config file
- whether automatic discovery of web servers would occur or not
- the path to the discovery config file
- whether automatic monitoring of web servers would occur or not
- the path to the custom metric configuration file to be used while monitoring. This is supported only for Apache and Apache based web servers.
- the truststore file path containing the web server certificates
- truststore password, in encrypted form, to unlock the truststore file

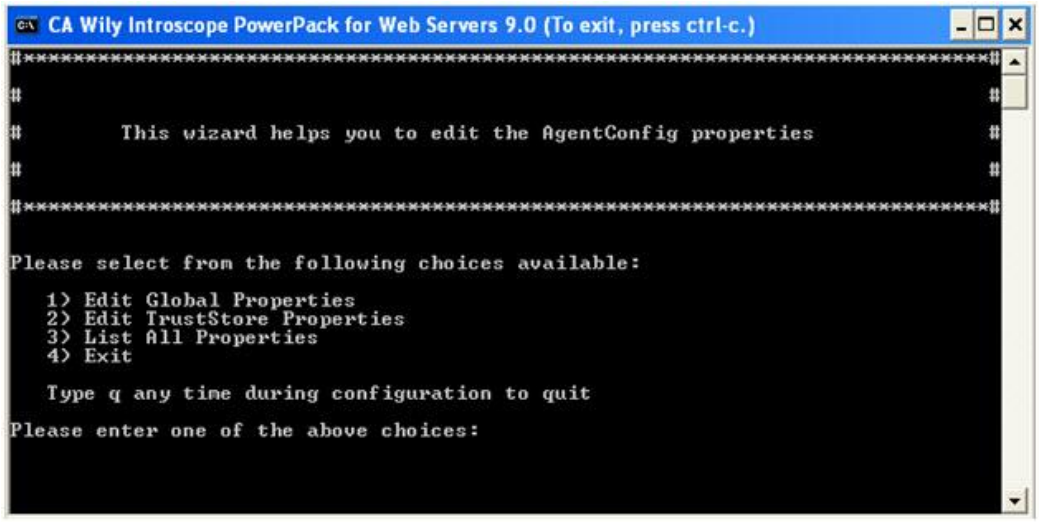
You must use *AgentConfigTool.bat* file to edit the *AgentConfig.properties* file.

If you are using default properties specified in *AgentConfig.properties* file, you need not execute the *AgentConfigTool.bat* file.

If your web server uses HTTPS in non-permissive mode, you must set the truststore path and truststore password for the valid certificates that are used to establish communication with the web server. To set the truststore settings, you must use *AgentConfigTool.bat* file to edit the *AgentConfig.properties* file. This ensures that the truststore password is stored in an encrypted form in the *AgentConfig.properties* file.

To configure the AgentConfig.properties file:

1. Double-click the *AgentConfigTool.bat* file to execute it. The command prompt window appears.



2. Select the property to edit:
   - To edit global properties, press 1 and ENTER.
   - To edit truststore properties, press 2 and ENTER.
   - To list both global and truststore properties, press 3 and ENTER.
3. You are prompted to enter values for each property.
   - Specify a new value for the property and press ENTER.
   - Press ENTER to set the default value for the property.
   - Press C and ENTER to preserve the existing value for the property.

   Note: For truststore path, if you enter an invalid path, you are asked to enter the correct path for two more times. If you fail to provide the correct path, the batch file terminates execution and the command prompt window closes. If you do not enter value for the truststore password, you are asked to enter a value for two more times. If you fail to provide a value for the password, the batch file terminates execution and the command prompt window closes.
4. To exit the command prompt, press 4 and ENTER.

Step 5: Configuring web servers to publish statistics

To see performance statistics for the web server in Introscope, you need to enable the publishing of statistics.

Publishing statistics on Apache and its derivatives

To publish performance statistics, you must enable and configure the Apache server_status module (mod_status).

To publish statistics on Apache and its derivatives:

1. Stop the web server.
2. Open the *httpd.conf* file present in the Apache or its derivatives' installation directory.
3. Enable the mod_status directive by uncommenting the directive line. The directive may be similar to the following line:
   ```
   #LoadModule status_module modules/mod_status.so
   ```
   Note: Perform this step only if *mod_status* is not already compiled into the web server. Otherwise, *module status_module is built-in and cannot be loaded* error message would be seen. Use *httpd -l* command to find out the modules which are already compiled into the web server.
4. Enable server status reports by uncommenting the lines of the Location configuration directives:
   ```
   <Location /server-status>
   SetHandler server-status
   Order deny,allow
   Deny from all
   Allow from .your_domain.com
   </Location>
   ```
   Note: If you are unable to find this block, manually add it.
5. To restrict access to the server-status output, define access to only the machine where you are running the CA APM for Web Servers. In the line *Allow from .your_domain.com*, replace *.your_domain.com* with the name of the machine running the CA APM for Web Servers. For example:
   ```
   Allow from jbacyzf-dt.wilytech.com
   ```
6. Uncomment the ExtendedStatus directive and ensure the ExtendedStatus property value is *On*:
   ```
   ExtendedStatus On
   ```
   Note: If you are unable to find this line, manually add it. When you enable extended status, additional metrics are obtained. See Apache/IHS/OHS metrics (see page 66) for details.
7. Save the *httpd.conf* file and restart the web server.
8. To test, start up a web browser on a machine allowed access to your server's server-status and point it at the following URL:
   ```
   http://<server-name>/server-status
   ```
   Note: The above URL is not hard coded. See Configurable statistics page location (see page 56) for details.

Publishing statistics for IIS 6.0 and 7.0

To publish statistics for IIS:

1. You must copy the *<PPWebServersHome>\IIS* directory to the machine where the IIS web server is running.

   IMPORTANT: Ensure that the following two WMI classes are available on the IIS web server machine. If the classes are not available, the *PublishIISStats.vbs* may crash and thus fail to retrieve IIS metrics. WMI classes:
   Win32_PerfFormattedData_InetInfo_InternetInformationServicesGlobal
   Win32_PerfFormattedData_W3SVC_WebService

2. Open the *IIS/VBScript.bat* file and update the file with the absolute path for the *IIS/PublishIISStats.vbs* file and the absolute path to publish stats page.

   For example,
   ```
   cscript /nologo "D:\PPWebServers\IIS\PublishIISStats.vbs"
   /output:"C:\InetPub\wily\iis-stats.html" /frequency:15
   ```

3. Double-click the *RegisterVBScriptService.bat* file to register the VBScript as windows service.

   Note: Refer to the *VBscript.log* file for any problems encountered while starting or stopping the IIS web server VB Script Service.

4. Create a new virtual directory called *IISPerfStats*. Set the default page for this virtual directory to the html page in 020; *iis-stats.html* in the example. Give only read permission to this virtual directory to ensure that it is completely secure.

   Note: The virtual directory is not hard coded. See Configurable statistics page location (see page 56) for details.

5. Click Start > Run. The Run dialog box appears.

6. Type *Services.msc* in the Open text box.

7. Click OK. A list of all Windows services appears.

8. Right-click IIS web server VB Script Service and click Start.

   CA APM for Web Servers starts picking up the required data for metrics from the stats page that you specified in the *VBScript.bat* file.

9. Right-click IIS web server VB Script Service and click Stop to stop the VB script from executing. CA APM for Web Servers also stops picking the required data for metrics.

To unregister the VB Script as Windows Service

- Double-click the *DeregisterVBScriptService.bat* file.

The VB Script gets unregistered as the Windows service.

Publishing statistics for Sun ONE

To publish statistics for Sun ONE:

1. Add the following object to your obj.conf file after the default object:
   ```
   <Object name="perf">
   Service fn="service-dump"
   </Object>
   ```
2. Add the following as the first line to the default object:
   ```
   NameTrans fn=assign-name from="/.perf" name="perf"
   ```
3. If not already enabled, enable statistics on the server. To enable statistics from the user interface, perform the following steps:
   a. From the Server Manager, select the Monitor tab.
   b. Select Monitor Current Activity. The Enable Statistics/Profiling page appears.
   c. Select Yes to enable.
   d. Click OK and Apply.
   e. Select Apply Changes to restart the server for your changes to take effect.

   For more information, refer to Sun ONE docs for instructions:
   http://docs.sun.com/source/816-5690-10/perf6.htm#16301
4. Restart the web server.
5. To test, start up a web browser on a machine allowed access to your server and point it at the URL:
   ```
   http://<server-name>/.perf
   ```
   Note: The above URL is NOT hard coded. See Configurable statistics page location (see page 56) for details.

Step 6: Defining web servers to monitor

There are two methods to let the CA APM for Web Servers know about the web servers that you want to monitor:

- Configure the CA APM for Web Servers to auto-discover web servers (see page 32).
- Manually configure the web servers to monitor in the *WebServerConfig.xml* file (see page 35).

(Optional) Configuring auto-discovery of web servers

To let the CA APM for Web Servers discover any web servers automatically, you must add the subnets to scan in the *DiscoveryConfig.xml* file and specify a scanning frequency. The CA APM for Web Servers scans the subnets at the specified frequency and if it finds web servers in the subnet, adds them to the list of web servers in the *WebServerConfig.xml* file. It also adds them to the Discovered Servers node list in the Investigator tree of the Introscope Workstation.

Note: Just because a web server has been discovered does not mean that it is monitored automatically. If you want the web servers that are automatically discovered to be monitored automatically, you must specify this in the *AgentConfig.properties* file.

Auto-discovery and auto-monitoring

Consider a case where you configure discovery over a particular subnet. If you introduce a new web server, later in this subnet, auto-discovery takes care of discovering the new web server, dynamically, without user intervention; provided the web server is supported and its port is already included in the subnets to scan in *DiscoveryConfig.xml*.

Auto-monitoring specifies the ability of the product to monitor the discovered web servers automatically and report the basic availability and information metrics to Introscope.

Once a web server is discovered, the CA APM for Web Servers only reports basic statistics such as IP address and port. In order to get more performance metrics, you must configure the web server to publish statistics. See Step 5: Configuring web servers to publish statistics (see page 28).

Note: For auto-discovery and auto-monitoring to work, you must set *agent.discovery = true* and *agent.automonitor=true* in *AgentConfig.properties* file.

To configure DiscoveryConfig.xml file:

1. Open the *config\DiscoveryConfig.xml* file.
2. Under the Add your subnets here section, define the subnets to scan for web servers.

   Note: If you are upgrading from version 1.0 or version 1.0.1.0, you have already added the subnet information as part of upgrade. Perform this step only if you want to change any subnet information or you may skip this step and perform the next step 3 for defining the ports.

   Each subnet can be mentioned as an IP/mask pair or a Range of IP. The subnet information should be enclosed within the tags *<SubNet>* and *</SubNet>*.

For example,
<SubNet>2002:4567::155.35.13.175-2002:4567::155.35.13.190
</SubNet>

There are various formats using which the subnets can be mentioned depending on whether the IP addresses to scan are IPv4 or IPv6. You can specify the subnet either as a range of IP addresses, subnet in Classless Inter-Domain Routing (CIDR) notation, or IP/subnetmask in dotted-mask notation which is valid only for IPv4 addresses. Please refer to the examples for the supported SubNet formats.

Examples of how subnets can be listed are outlined in the following section.

- Range of IPv6 addresses presented in expanded format

  Example:
  <SubNet>2002:4567:cfd:aef:cdb:abc:ff:e0-2002:4567:cfd:aef:cdb:abc:ff:f0</SubNet>

- Range of IPv6 addresses in compressed form

  Example:
  <SubNet>2002:4567:defc:abcd::cebc-2002:4567:defc:abcd::cecf</SubNet>

- Range of IPv4 addresses

  Example: *<SubNet>155.35.88.56-155.35.88.80</SubNet>*

- Range of IPv6 addresses represented using an IPv4-ended-IPv6 notation

  Example:
  <SubNet>2002:4567::172.34.67.34-2002:4567::172.34.67.90</SubNet>

- CIDR notation of IPv4 addresses

  Example: *<SubNet>172.34.67.34/24</SubNet>*

- CIDR notation of IPv6 addressesIPv6 address can be an expanded or compressed one apart from the IPv4-ended one specified

  Example: *<SubNet>2002:4567::155.35.14.0/126</SubNet>*

- Traditional IPv4 format of specifying a subnet in dotted-mask notation

  Example: *<SubNet>172.34.67.34/255.255.255.0</SubNet>*

IMPORTANT: Depending on the number of hosts to scan, Discovery may run for a long time. This is due to the fact that the number of hosts in IPv6 address space can go up to 2^64.

3. Define the ports to scan for under the Add your ports here section.

   Note: If you are upgrading from version 1.0 or version 1.0.1.0, you have the *PortNumber* and *Type* information as part of upgrade. However, you need to explicitly add the *<FingerPrintMatcher>* tags for the appropriate web servers, as shown in the example.

   For the discovery to occur over HTTP, specify the Port Number, Type, and Web Servers. For example,

```
<Port Number="80" Type="TCP" >
<FingerPrintMatcher>Apache</FingerPrintMatcher>
<FingerPrintMatcher>Apache:IBM_HTTP_SERVER</FingerPrintMatcher>
<FingerPrintMatcher>Apache:Oracle-HTTP-Server
</FingerPrintMatcher>
<FingerPrintMatcher>Microsoft-IIS</FingerPrintMatcher>
<FingerPrintMatcher>Sun-ONE</FingerPrintMatcher>
<FingerPrintMatcher>Sun-ONE:Netscape-Enterprise
</FingerPrintMatcher>
</Port>
```

4. For the discovery to occur over HTTPS, you must specify the Port Number, Type, Protocol, Mode, and Web Servers. Protocol must either be SSL or TLS. Mode must be either Permissive or Non-Permissive.

   Note: If you are upgrading from version 1.0 or version 1.0.1.0, you have the *PortNumber* and *Type* information as part of upgrade. However, you need to explicitly add information for *Protocol*, *Mode*, and the *<FingerPrintMatcher>* tags for the appropriate web servers, as shown in the example.

   For example,

```
<Port Number="443" Type="TCP" Protocol="SSL"
Mode="Non-Permissive">
<FingerPrintMatcher>Apache</FingerPrintMatcher>
<FingerPrintMatcher>Apache:IBM_HTTP_SERVER</FingerPrintMatcher>
<FingerPrintMatcher>Apache:Oracle-HTTP-Server
</FingerPrintMatcher>
<FingerPrintMatcher>Microsoft-IIS</FingerPrintMatcher>
<FingerPrintMatcher>Sun-ONE</FingerPrintMatcher>
<FingerPrintMatcher>Sun-ONE:Netscape-Enterprise
</FingerPrintMatcher>
</Port>
```

   Note: If you use Non-Permissive mode to connect to the web servers over HTTPS, then you must specify TrustStore properties by running the *AgentConfigTool.bat* file. If you do not do so, auto discovery and auto monitoring of webservers fails.

5. Specify the scanning frequency in the *<Schedule> </Schedule>* element. The default scanning frequency is 30 minutes.
6. Specify the concurrency value in the *<Concurrency> </Concurrency>* element. The default concurrency value is 10 threads. You may increase this to enable faster network scans.
7. If you want the discovered web servers to be reported to the Enterprise Manager, set the *<ReportToEM>* element to true.
   `<ReportToEM> true <ReportToEM>`
8. Save changes to the *DiscoveryConfig.xml* file.

Manually configuring the CA APM for Web Servers

It is recommended that you let the CA APM for Web Servers auto-discover web servers on your subnet, as this process adds web server details to the list in the WebServerConfig.xml file. However, you can also define web servers manually in the *WebServerConfig.xml* file. You can also edit discovered web servers' details in this file. This file is polled by the CA APM for Web Servers every 60 seconds, so that the changes are picked up quickly.

To define web servers manually or edit web server details:

1. Open the *WebServerConfig.xml* file.
2. Under the Add your web servers here section, add a line for each web server to monitor, filling in the web servers details:

   Note: If you are upgrading from version 1.0 or version 1.0.1.0, you have already added the web servers information as part of upgrade. Perform this step only if you want to change any web servers information or you may skip this step.

   - WebServer Type—Base and its variant for each web server type found in the *WebServerConfig.xml* file.
   - Enabled—whether monitoring is enabled. Values accepted are *true* or *false*. If set to true, monitoring is enabled.
   - Protocol—specify the protocol that is used to communicate with the web server; the protocol used is either SSL (Secure Sockets Layer) or TLS (Transport Layer Security). Default Protocol used is SSL.
   - Mode—specify the mode that the CA APM for Web Servers uses to communicate with the web server using the HTTPS protocol. Default value is Non-Permissive.
   - ServerURL—URL of web server to be monitored.
   - DisplayName—Display name of the web server in the Introscope Investigator tree.

- RefreshFrequencyInSeconds—how often the CA APM for Web Servers fetches statistics from a web server. The default is 15 seconds.
- MetricsURL—specify the customized stats page location in the Metrics URL. For a web server that is configured to publish its metrics in a customized stats page location, specify the customized stats page location in the Metrics URL.

For example, the following lines would monitor an Oracle HTTP Server based on Apache, that uses HTTPS protocol in a non-permissive mode with a 30-second refresh frequency:

```
<WebServer Type="Apache:Oracle-HTTP-Server" Enabled="true" Protocol="SSL"
Mode="Non-Permissive"
ServerURL="https://xyzabc:443" DisplayName="xyzabc-Apache"
RefreshFrequencyInSeconds="30"/>
```

Note: Make sure there are no ":" and "|" characters in the DisplayName property, as they will cause incorrect Metric name formatting.

Consider that you want to monitor a web server running in an IPv6 environment by specifying its URL with IPv6 address. In accordance with the standard convention, you must enclose the IPv6 address in square brackets. The following code monitors an Apache web server, that uses HTTP protocol, running in IPv6 environment with a 30-second refresh frequency:

```
<WebServer Type="Apache" Enabled="true"
ServerURL="http://[2002:4567:defc:abcd::cebc]:80" DisplayName="IPv6-Apache"
RefreshFrequencyInSeconds="30"/>
```

Note: If you specify the URL of a web server running in IPv6 environment with its name instead of its IPv6 address, do not enclose the name in square brackets.

3. Save changes to the *WebServerConfig.xml* file.

Step 7: Enabling the Management Module and dashboards

The Management Module contains pre-configured dashboards for each web server type. The Enterprise Manager installer placed the files in the *<IntroscopeHome>\examples* directory. To enable the dashboards, you must move the Management Module file to the directory where the Enterprise Manager will recognize it.

To install the Management Module on the Enterprise Manager Machine:

1. Copy the Management Module file, *PPWebServers_ManagementModule.jar*, located in

   <IntroscopeHome>\examples\PowerPackForWebServers\config\modules

   to the <IntroscopeHome>\config\modules directory in the Enterprise Manager's installation directory.

2. Restart the Enterprise Manager to recognize the new Management Module.

Step 8: (Optional) Customizing ApacheCustomMetrics.xml file

Note: Perform the following steps only if you have Apache or Apache-based web servers and have customized the metrics, that is, changed the metric name or metric units for those web servers.

To customize ApacheCustomMetrics.xml file:

1. Open *ApacheCustomMetrics.xml* file.
2. In the *<CustomMetrics>* element, add entries for metrics that have been customized for Apache and Apache-based web servers. This helps the CA APM for Web Servers to display the correct data for the metrics.

   Note: You may use divisor and multiplier integer values.

   For example, if you have customized the *Total Accesses* metrics to be displayed as *Total kHits*, enter the following lines in the file:

   ```
   <Metric name="Total Accesses">
   <Alias name="Total kHits" multiplier="1000"/>
   </Metric>
   ```

   Note: You need to multiply *Total kHits* by 1000 to display the correct data.

   If you have customized the *Total kBytes* metrics to be displayed as *Total Bytes*, enter the following lines in the file:

   ```
   <Metric name="Total kBytes">
   <Alias name="Total Bytes" divisor="1024"/>
   </Metric>
   ```

   Similarly, if you have customized *IdleWorkers* as *IdleLabours*, add the following lines in the file:

   ```
   <Metric name="IdleWorkers">
   <Alias name="IdleLabours"/>
   </Metric>
   ```

3. Save and close the *ApacheCustomMetrics.xml* file.

Step 9: Starting the CA APM for Web Servers on Windows

To run the CA APM for Web Servers:

1. Click Start > Run. The Run dialog box appears.
2. Type *Services.msc* in the Open text box.
3. Click OK. A list of all Windows services appears.
4. Right-click CA APM for Web Servers for Web Servers - Agent and click Start.

5. The CA APM for Web Servers starts and discovers or monitors web servers in one of the following ways based on how you have configured the *agent.discovery* and *agent.automonitor* properties in *AgentConfig.properties* file:
   - Auto-discover and auto-monitor web servers configured in the *DiscoveryConfig.xml* file if *agent.discovery=true* and *agent.automonitor=true*.
   - Only auto-discover web servers configured in the *DiscoveryConfig.xml* file if *agent.discovery=true* and *agent.automonitor=false*.
   - Start without auto-discovery and only monitor web servers configured in *WebServerConfig.xml* file if *agent.discovery=false*.

Note: Refer to .*logs**WSPPService.log* file for any problems encountered while starting or stopping the CA APM for Web Servers.

You have now completed the installation for CA APM for Web Servers.

Step 10: Stopping the CA APM for Web Servers on Windows

To stop the CA APM for Web Servers:

1. Click Start > Run. The Run dialog box appears.
2. Type *Services.msc* in the Open text box.
3. Click OK. A list of all Windows services appears.
4. Right-click CA APM for Web Servers - Agent and click Stop.

   CA APM for Web Servers stops running.

Step 11: Unregistering the CA APM for Web Servers as a Windows service

- Double-click the *DeregisterWSService.bat* file in the *<PPWebServersHome>* directory.

This unregisters the CA APM for Web Servers as a Windows Service.

Note: Refer to .*logs**WebServerAgent.log* file for information regarding all operations for CA APM for Web Servers from the time you started it till the CA APM for Web Servers agent is stopped or shutdown. The *WebServerAgent.log* file is created automatically in the *./logs* folder once you start the CA APM for Web Servers through the Windows service.

Installing CA APM for Web Servers components on UNIX

Installing and configuring the CA APM for Web Servers on UNIX involves the following steps:

Step 1: Running the main Enterprise Manager installer on UNIX (see page 39)

Step 2: Installing CA APM for Web Servers agent components on UNIX (see page 40)

Step 3: Configuring the AgentConfig.properties file on UNIX (see page 41)

Step 4: Configuring web servers to publish statistics (see page 42)

Step 5: Defining web servers to monitor (see page 43)

Step 6: Enabling the Management Module and dashboards (see page 43)

Step 7: (Optional) Customizing ApacheCustomMetrics.xml file (see page 43)

Step 8: Starting the CA APM for Web Servers on UNIX (see page 43)

Step 9: Stopping the CA APM for Web Servers on UNIX (see page 44)

Step 10: Optional: Restarting the CA APM for Web Servers or finding its status on UNIX (see page 44)

Step 1: Running the Enterprise Manager installer on UNIX

Run the Enterprise Manager installer to install the CA APM for Web Servers along with the Enterprise Manager. The Enterprise Manager installer places the files into the *<IntroscopeHome>/examples/PowerPackForWebServers* directory. You will later move the files to the correct location, based on how they are organized in the */examples* directory.

For details about the main installer and where to find the installer executable, see the *CA APM Installation and Upgrade Guide*.

The Enterprise Manager installer places the following files onto the Enterprise Manager machine:
<IntroscopeHome>/examples/PowerPackForWebServers/config/modules/PPWebServers_ManagementModule.jar

This file is the CA APM for Web Servers Management Module, which contains pre-configured dashboards.

Step 2: Installing CA APM for Web Servers agent components on UNIX

Run the Standalone agent installer to install and initially configure the CA APM for Web Servers agent information. This installer configures the agent with the Enterprise Manager host and port number.

Although the CA APM for Web Servers does not install an agent on the web server to collect web server data, it uses Introscope agent to report the data back to the Enterprise Manager.

The configuration changes to the *WebServerAgent.profile* file on UNIX are the same as for the *WebServerAgent.profile* file on Windows. See Step 2: Installing CA APM for Web Servers agent components on Windows (see page 24).

The CA APM for Web Servers agent files on UNIX

The Enterprise Manager installer places the following files on the agent machine in the *<PPWebServersHome>* directory:

AgentConfigTool.sh

Shell script file that configures the global and truststore settings for agent.

ServerVersionFinder.sh

Shell script file to find server header of a given HTTP or HTTPS web server URL.

UpdateMonitorConfigFile.sh

Shell script file to upgrade the old WebServerConfig.xml to the new format.

WebServerMonitor.sh

Shell script file to start, stop, or restart the CA APM for Web Servers.

./config/AgentConfig.properties

Properties for CA APM for Web Servers agent. Use the AgentConfigTool.bat file to set these properties.

./config/ApacheCustomMetrics.xml

Customizable file to map customized metric list to standard metric list. This is applicable to only Apache web server and web servers based on Apache.

./config/DiscoveryConfig.xml

Configuration file to specify which subnets to scan for web servers.

./config/WebServerAgent.profile

Profile for web server agent.

./config/WebServerConfig.xml

Configuration file to specify which web servers to monitor.

./lib/commons-logging-1.1.jar

A dependent JAR file for the CA APM for Web Servers agent.

./lib/jline-0.9.9.jar

JAR file used to mask the truststore password.

./lib/PPWebServers.jar

CA APM for Web Servers JAR file.

./lib/WebServerAgent.jar

Introscope web server agent; communicates web server statistics to Enterprise Manager.

./lib/commons-codec-1.3.jar

A dependent JAR file for CA APM for Web Servers agent.

./lib/ext/Supportability-Agent.jar

Introscope agent extension used for debugging by CA Support.

Step 3: Configuring the AgentConfig.properties file on UNIX

You can specify the global settings for the CA APM for Web Servers in the *AgentConfig.properties* file. This file has the following properties:

- the path to the Web Server Config file
- whether automatic discovery of web servers would occur or not
- the path to the discovery config file
- whether automatic monitoring of web servers would occur or not
- the path to the custom metric configuration file to be used while monitoring. This is supported only for Apache and Apache based web servers.
- the truststore file path containing the web server certificates
- truststore password, in encrypted form, to unlock the truststore file

You must use *AgentConfigTool.sh* file to edit the *AgentConfig.properties* file.

If you are using default properties specified in *AgentConfig.properties* file, you need not execute the *AgentConfigTool.sh* file.

If your web server uses HTTPS in non-permissive mode, you must set the truststore path and truststore password for the valid certificates that are used to establish communication with the web server. To set the truststore settings, you must use *AgentConfigTool.sh* file to edit the *AgentConfig.properties* file. This ensures that the truststore password is stored in an encrypted form in the *AgentConfig.properties* file.

To configure the AgentConfig.properties file:

1. Execute *./AgentConfigTool.sh* from the console. The different options to edit the *AgentConfig.properties* file are displayed.
2. Select the property to edit:
   - To edit global properties, press 1 and ENTER.
   - To edit truststore properties, press 2 and ENTER.
   - To list both global and truststore properties, press 3 and ENTER.
3. You are prompted to enter values for each property.
   - Specify a new value for the property and press ENTER.
   - Press ENTER to set the default value for the property.
   - Press C and ENTER to preserve the existing value for the property.

   Note: For truststore path, if you enter an invalid path, you are asked to enter the correct path for two more times. If you fail to provide the correct path, the Shell script file terminates execution. If you do not enter value for the truststore password, you are asked to enter a value for two more times. If you fail to provide a value for the password, the Shell script file terminates execution.
4. To exit the command prompt, press 4 and ENTER.

Step 4: Configuring web servers to publish statistics

To see performance statistics for the web server in Introscope, you need to enable the publishing of statistics.

More information:

Step 5: Configuring web servers to publish statistics (see page 28)

Step 5: Defining web servers to monitor

The procedure to define Web servers to monitor on UNIX is same as the procedure define Web servers to monitor on Windows.

More information:

Step 6: Defining web servers to monitor (see page 31)

Step 6: Enabling the Management Module and dashboards

The procedure to enable Management Modules on UNIX is same as the procedure to enable Management Modules on Windows.

More information:

Step 7: Enabling the Management Module and dashboards (see page 36)

Step 7: (Optional) Customizing ApacheCustomMetrics.xml file

The procedure to customize *ApacheCustomMetrics.xml* file on UNIX is same as the procedure to customize *ApacheCustomMetrics.xml* file on Windows.

More information:

Step 8: (Optional) Customizing ApacheCustomMetrics.xml file (see page 37)

Step 8: Starting the CA APM for Web Servers on UNIX

To run the CA APM for Web Servers:

1. On the command line prompt, type the following line and press ENTER:
   `./WebServerMonitor.sh start`

   IMPORTANT: When the CA APM for Web Servers starts, the process ID of the CA APM for Web Serversagent is stored in the pids directory. Do not delete this directory or its contents. If you delete the directory, the current status of the CA APM for Web Servers is lost.

2. The CA APM for Web Servers starts and discovers or monitors web servers in one of the following ways based on how you have configured the *agent.discovery* and *agent.automonitor* properties in *AgentConfig.properties* file:
   - Auto-discover and auto-monitor web servers configured in the *DiscoveryConfig.xml* file if *agent.discovery=true* and *agent.automonitor=true*.
   - Only auto-discover web servers configured in the *DiscoveryConfig.xml* file if *agent.discovery=true* and *agent.automonitor=false*.
   - Start without auto-discovery and only monitor web servers configured in *WebServerConfig.xml* file if *agent.discovery=false*.

Note: Refer to *.\logs\WebServerAgent.log* file for any problems encountered while starting or stopping the CA APM for Web Servers.

You have now completed the installation for CA APM for Web Servers.

Step 9: Stopping the CA APM for Web Servers on UNIX

- On the command line prompt, type the following line and press ENTER:
  `./WebServerMonitor.sh stop`

The CA APM for Web Servers stops running.

Step 10: (Optional) Restarting the CA APM for Web Servers or finding its status on UNIX

- On the command line prompt, type the following line and press ENTER:
  `./WebServerMonitor.sh status`

This command gives the current status of the agent extension.

- On the command line prompt, type the following line and press ENTER:
  `./WebServerMonitor.sh restart`

This command stops and starts the agent extension.

Note: Refer to *.\logs\WebServerAgent.log* file for information regarding all operations for extension from the time you started it till the agent extension is stopped or shutdown. The *WebServerAgent.log* file is created automatically in the *./logs* folder once you start the extension by executing the shell script *WebServerMonitor.sh* file in UNIX.

Upgrading the CA APM for Web Servers

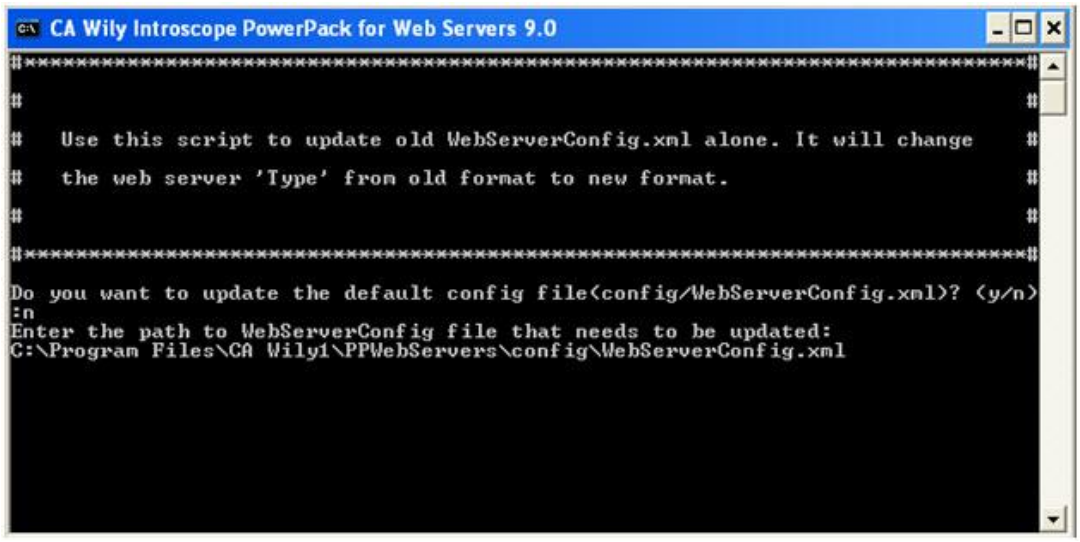
The Enterprise Manager installer does not upgrade from previous versions, rather it is a manual process that primarily involves backing up your installation and using the Enterprise Manager installer to install the current version.

To upgrade the CA APM for Web Servers:

1. Take a back up of your *WebServerConfig.xml* and *DiscoveryConfig.xml* files from your existing CA APM for Web Servers directory.
2. Run the Standalone agent installer to install the current version.
3. Copy the *<SubNet>* and *CA Portal* information from old backed-up *DiscoveryConfig.xml* to the new file from the Enterprise Manager installer. Note that the attributes for the *<FingerPrintMatcher>* element have been changed in this release. So, while copying the *CA Portal* information, ensure that you only copy the port numbers and their types to the new file. See Configuring auto-discovery of web servers (see page 32) for details
4. Copy the valid *<WebServer>* information from old backed-up *WebServerConfig.xml* to the new one.

   Note: Ensure that you do not copy the comments.
5. For Windows, double-click the *UpdateMonitorConfigFile.bat* file to execute it. The command prompt window appears. For UNIX, in the console type *./UpdateMonitorConfig.sh* and press ENTER. You are asked whether you want to update the *WebServerConfig.xml* file in the default location or not.

   This figure shows the *UpdateMonitorConfigFile.bat* script being executed on Windows.



6. If you type *y* and press ENTER, the batch file upgrades the web server definitions from the old format to the new format. The updates are done to the *WebServerConfig.xml* file present in the *<PPWebServersHome>/config* directory. For example,

   If in an earlier version the web server type was *IBM_HTTP_Server/2.0*, in the new version it is changed to *Apache:IBM_HTTP_Server*.

   Note: Press *y* only if the web server definitions from the old backed-up file were copied to *WebServerConfig.xml* in Step 4.

7. If you type *n* and press ENTER, the batch file asks for the path to the *WebServerConfig.xml* file, for which you want to update the format from old to new. After validating the path you entered, the script will update the specified file.

   Note: The modifications made by the update script are limited to changing the web server type from the old to the new format.

8. To configure the new CA APM for Web Servers on Windows, see Installing CA APM for Web Servers components on Windows (see page 23). To configure the new CA APM for Web Servers on UNIX, see Installing CA APM for Web Servers components on UNIX (see page 39).

Upgrading from an earlier version

To upgrade the CA APM for Web Servers from version 1.0:

1. Take a back up of your *WebServerConfig.xml* and *DiscoveryConfig.xml* files from your existing CA APM for Web Servers directory.
2. Install the new files.
3. Open the old, backed-up *DiscoveryConfig.xml* file. If you have mentioned any subnets to scan, using the following format:

   ```
   <SubNet>
   <IPAddress>172.34.54.67</IPAddress>
    <Mask>255.255.255.0</IPAddress>
   </SubNet>
   ```

   Change this to:

   ```
   <SubNet>172.34.54.67/255.255.255.0</SubNet>
   ```

   Note: The tags *<IPAddress>* and *<Mask>* are removed and you have to use the *<SubNet>* tag only.

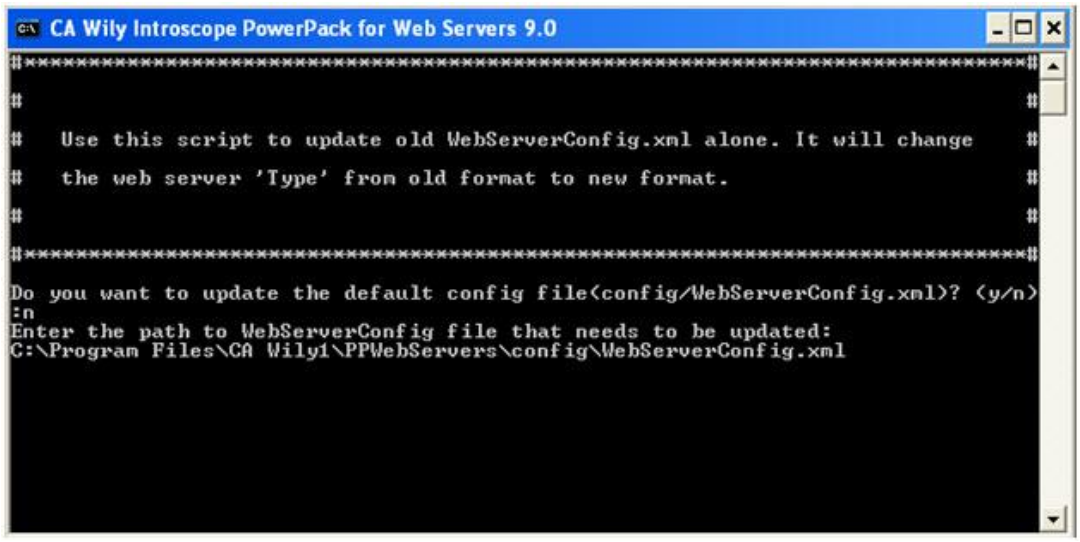
4. Copy all the port information from the old, backed-up *DiscoveryConfig.xml* file to the new *DiscoveryConfig.xml* file and save the changes done to the new file. Note that the attributes for the <*FingerPrintMatcher*> element have been changed in this release. So, while copying the *CA Portal* information, ensure that you only copy the port numbers and their types to the new file. For more information, see Configuring auto-discovery of web servers (see page 32).

5. Copy the valid <*WebServer*> information from old backed-up *WebServerConfig.xml* to the new one.

   Note: Ensure that you do not copy the comments.

6. For Windows, double-click the *UpdateMonitorConfigFile.bat* file to execute it. The command prompt window appears. For UNIX, in the console type *./UpdateMonitorConfig.sh* and press ENTER. You are asked whether you want to update the *WebServerConfig.xml* file in the default location or not.

   This figure shows the *UpdateMonitorConfigFile.bat* script being executed on Windows.



If you type *y* and press ENTER, the batch file upgrades the web server definitions from the old format to the new format. The updates are done to the *WebServerConfig.xml* file present in the *<PPWebServersHome>/config* directory. For example,

If in the previous version the web server type was *IBM_HTTP_Server/2.0*, in the new version it is changed to *Apache:IBM_HTTP_Server*.

Note: Press *y* only if the web server definitions from the old backed-up file were copied to *WebServerConfig.xml* in Step 4.

7. If you type *n* and press ENTER, the batch file asks for the path to the *WebServerConfig.xml* file, for which you want to update the format from old to new. After validating the path you entered, the script will update the specified file

   Note: The modifications made by the update script are limited to changing the web server type from the old to the new format.

8. To configure the new CA APM for Web Servers on Windows, see Installing CA APM for Web Servers components on Windows (see page 23). To configure the new CA APM for Web Servers on UNIX, see Installing CA APM for Web Servers components on UNIX (see page 39).

Chapter 3: Using the CA APM for Web Servers

This section describes how to effectively use the features in this version of the CA APM for Web Servers.

This section contains the following topics:

HTTPS support (see page 49)
Improved support for web servers (see page 51)
Changing Per Second Metrics to Per Interval (see page 55)
Configurable statistics page location (see page 56)

HTTPS support

The CA APM for Web Servers provides the capability to discover and monitor web servers over HTTPS protocol.

The CA APM for Web Servers can discover and monitor web servers communicating over HTTPS. SSL v3.0 and TLS v1.0 are supported. SSL v2.0 and PCT v1.0 are not supported.

The CA APM for Web Servers can be configured to work in two different modes: Permissive or Non-Permissive.

In the permissive mode, the CA APM for Web Servers acts as a permissive client that accepts all kinds of web server certificates. This includes unsigned, self-signed, trusted, and expired certificates.

In the non-permissive mode, the CA APM for Web Servers accepts only unexpired and trusted certificates. To configure this mode, the web server certificate must be made available by importing it into a trust store file on the machine where the CA APM for Web Servers is installed. If the CA APM for Web Servers is configured to discover or monitor a number of web servers over HTTPS in this mode, web server certificates from all these web servers must be imported into a trust store file.

The CA APM for Web Servers can be configured to communicate with the web server over SSL v3.0 or TLS v1.0 in both the modes. The protocol must be chosen depending upon the web server configuration.

The following additional attributes are needed to configure the CA APM for Web Serversto work in HTTPS:

- Protocol – Defines the protocol over which the CA APM for Web Servers tries to communicate with the web server. Default is SSLv3.0.
- Mode – Defines the mode in which the CA APM for Web Servers communicates with the web server. Supported modes are Permissive and Non-Permissive. Default mode is Non-Permissive. If the default mode is used, truststore settings must be provided in the *AgentConfig.properties* file using *AgentConfigTool.bat* file.

Note: In Non-Permissive mode, web servers with expired certificates are not monitored; even if the certificate is added to truststore file.

IMPORTANT: Only the cipher suites which are supported by Sun JRE 1.4.x and above are supported by the CA APM for Web Servers. See CA APM for Web Servers CipherSuites (see page 79) for details. This CA APM for Web Servers supports only X.509 Public Key Infrastructure Certificate formats.

To configure the CA APM for Web Servers to discover and monitor the web servers that are configured to communicate over HTTPS:

1. If you want to auto-discover and auto-monitor web servers that implement HTTPS, see Configuring auto-discovery of web servers (see page 32) to configure the *DiscoveryConfig.xml* file.
2. If you want to start without auto-discovering and only monitor web servers, see Manually configuring the CA APM for Web Servers to monitor web servers (see page 35) to configure the *WebServerConfig.xml* file.
3. If you use Non-Permissive mode, you must:
   a. Copy the certificates from web server machine to the machine where the CA APM for Web Servers agent is installed.
   b. Import the certificates to truststore. At the command prompt, type the following command and press ENTER.
   keytool –import –alias <alias name to the certificate> –file <path of the certificate> –keystore <name of truststore file> –storepass <password>

   This command imports the certificate defined with the *-file* option in the truststore defined with *-keystore* option. In case multiple web servers have been configured for discovery or monitoring over HTTPS, web server certificates from each of the web server must be imported into the truststore file.

The truststore password specified while configuring the truststore settings for the CA APM for Web Servers must match the password specified with the *-storepass* option in the keytool command.

Note: Keytool is a key and certificate management utility that comes with Sun JRE.

c. Specify TrustStore properties, otherwise monitoring and auto discovery fail. For windows, see Step 4: Configuring the AgentConfig.properties file on Windows (see page 27). For UNIX, see Step 3: Configuring the AgentConfig.properties file on UNIX (see page 41).

Improved support for web servers

This CA APM for Web Servers includes support for Oracle HTTP Server and all new base versions of Apache, Microsoft IIS, and Sun ONE web servers along with their variants.

Additionally, this feature supports the users' plug and play web servers that are not supported out of the box. The feature is available for discovery as well as monitoring. You also have an option to configure the discovery and monitoring of

- A new web server that's based on Apache web server and
- New releases of IIS and Sun ONE web servers.

In order to configure a new web server for discovering, the *FingerPrintMatcher* element has now changed. The *FingerPrintMatcher* element must contain information about the web server to discover in the *base:variant* format. Here the base defines the base web server over which the variant is built. You must specify the *FingerPrintMatcher* element in the following format in the *DiscoveryConfig.xml* file:

```
<Port Number="443" Type="TCP" Protocol="SSL"
Mode="Non-Permissive">
<FingerPrintMatcher>Apache</FingerPrintMatcher>
<FingerPrintMatcher>Apache:IBM_HTTP_SERVER</FingerPrintMatcher>
<FingerPrintMatcher>Apache:Oracle-HTTP-Server
</FingerPrintMatcher>
</Port>
```

In order to configure a new web server for monitoring, the web server type must be specified in the following format in the *WebServerConfig.xml* file:

```
<WebServer Type="base:variant">
```

Here, variant is a part of server response header returned by the web server and base defines the base web server over which the variant is built.

For example, Oracle-HTTP-Server is a variant of Apache base web server and must be defined in *WebServerConfig.xml* file as follows:

```
<WebServer Type="Apache:Oracle-HTTP-Server">
```

If you are not aware of the variant name of a particular web server, that is based on either Apache, Microsoft IIS, or Sun ONE, use *ServerVersionFinder.bat* for Windows or *ServerVersionFinder.sh* for UNIX or Linux to find the Server Header of a given HTTP or HTTPS Server.

To find the Server Header of a given HTTP or HTTPS Server:

1. Open a command prompt for Windows or console for UNIX or Linux and navigate to the directory where the *ServerVersionFinder* file resides.
2. Type the name of the batch or shell script file and press ENTER.

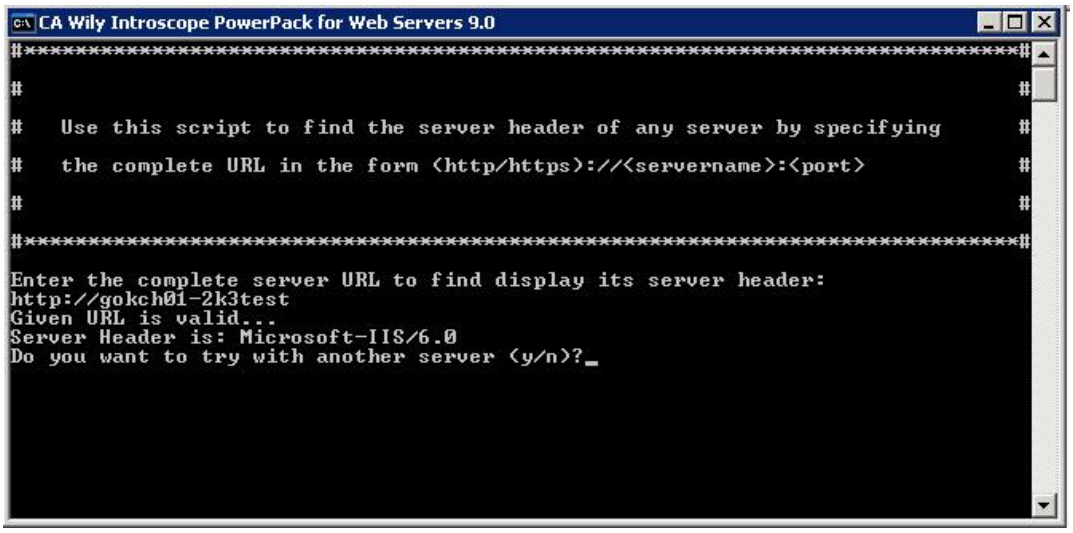
   You are prompted to enter the complete URL to access the web server for which you want to find the server header.
3. Type the complete URL and press ENTER.

   For example, *http://Wily-Apache-New:88*

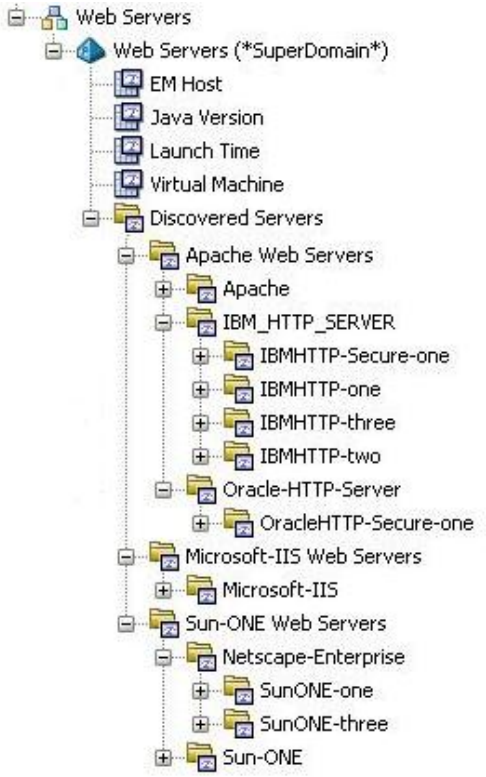
   The command window or console displays the Server Header of the web server.

   Note: The Server Header of a web server is available only if the URL you have entered is valid and accessible.

The following illustration is an example of how the *ServerVersionFinder.bat* or *ServerVersionFinder.sh* file is executed.



In the Investigator tree, under Discovered Servers and Monitored Servers node, you see an expandable node for the base server type. Under this node, you see all the variants based on the base server. The Investigator tree now looks as follows:



Note: The server version such as Apache 1.3 web servers is not displayed in the investigator tree; but you can always get the version information under Info metrics of the web server.

The CA APM for Web Servers also supports customized metrics for Apache and Apache based web servers.

More information:

Step 8: (Optional) Customizing ApacheCustomMetrics.xml file (see page 37)

Changing Per Second Metrics to Per Interval

The metrics for various web servers are reported on a per-interval basis rather than per second basis.

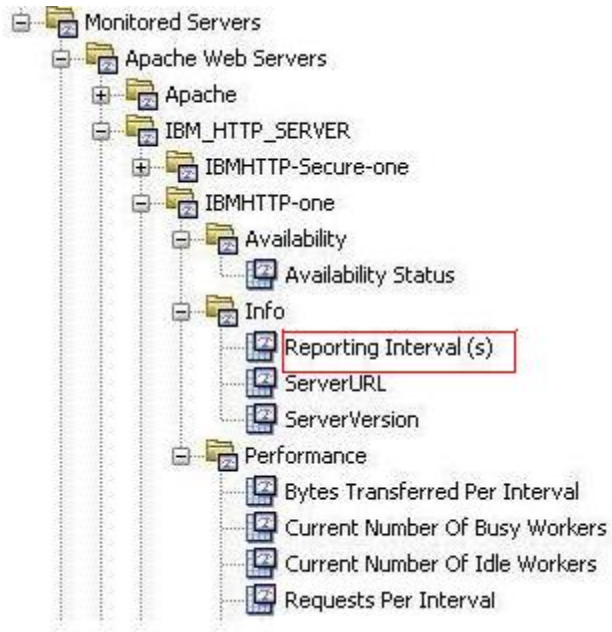
This feature is inline with most Introscope metrics that are based on interval and not second. Also, if the per second metrics' data is in fraction, the data is displayed as zero value. This can be misleading. In such cases, per-interval metrics helps in solving the problem.

To implement this feature, the interval parameter is now configurable.

To specify a reporting interval, manually add the attribute *RefreshFrequencyInSeconds* to <*WebServer*> tag and set it to the required value in *WebServerConfig.xml*.

Note: *RefreshFrequencyInSeconds* attribute is specific to each web server. For web servers where this attribute is not mentioned, the default of 15 seconds is taken.

Reporting of all per second metrics is now changed to per interval metrics. The new metric *Reporting Interval (s)* is added as part of this feature. This metric is shown under Info node for all monitored web servers. The value for this metric corresponds to the value of the *RefreshFrequencyInSeconds* attribute specified for that web server in the *WebServerConfig.xml* file.



For example, for an Apache web server with reporting interval of 60 seconds, the entry in *WebServerConfig.xml* file look as follows:

```
<WebServer Type="Apache" ServerURL="http://W-Apache" DisplayName="W-Apache-60sec"
RefreshFrequencyInSeconds="60"/>
```

Configurable statistics page location

You can configure the location of the HTML file used to publish web server statistics, for any supported web server.

By default, the CA APM for Web Servers looks for the web server statistics at the following locations: *server-status* for Apache, *iisperfstats* for Microsoft IIS, and *.perf* for Sun ONE.

If the web server has been configured to publish its statistics at a location different from the default locations, use the attribute *MetricsURL* in the *WebServerConfig.xml* to specify the new location. This attribute must be configured for each web server separately in the *WebServerConfig.xml* file. Also, the path is relative to the root path.

Note: The discovery process does not detect the stats page location. If a web server is configured to publish its statistics at a location different from the default location and the web server has been discovered by the CA APM for Web Servers, the web server gets added to the *WebServerConfig.xml* file without the *MetricsURL* attribute. For this web server, you must specify the correct *MetricsURL* so that the performance metrics are obtained.

Consider an Apache server W-Apache which is configured to publish its metrics in a page called *apachestats*. You must add the *MetricsURL* attribute corresponding to this server entry in *WebServerConfig.xml* as follows:

```
<WebServer Type="Apache" ServerURL="http://W-Apache" DisplayName="W-Apache"
MetricsURL="apachestats"/>
```

Similarly, the virtual directory name we create in IIS is customizable and must be mentioned in *MetricsURL* attribute. Consider another HTTPS enabled IIS server, running on port 445 with virtual directory customized to '*ssliisstats*'. The corresponding entry in *WebServerConfig.xml* must be as follows:

```
<WebServer Type="Microsoft-IIS" ServerURL="https://X-IIS:445" Protocol="ssl"
Mode="permissive" DisplayName="X-IIS" MetricsURL="ssliisstats"/>
```

Chapter 4: Viewing data from the CA APM for Web Servers

This chapter describes how to effectively use the Introscope Workstation to view web server data and diagnose web server problems.

This section contains the following topics:

Using the CA APM for Web Servers with Introscope Workstation (see page 57)
Viewing web server metrics in the Introscope Investigator tree (see page 58)
Viewing the CA APM for Web Servers dashboards (see page 60)

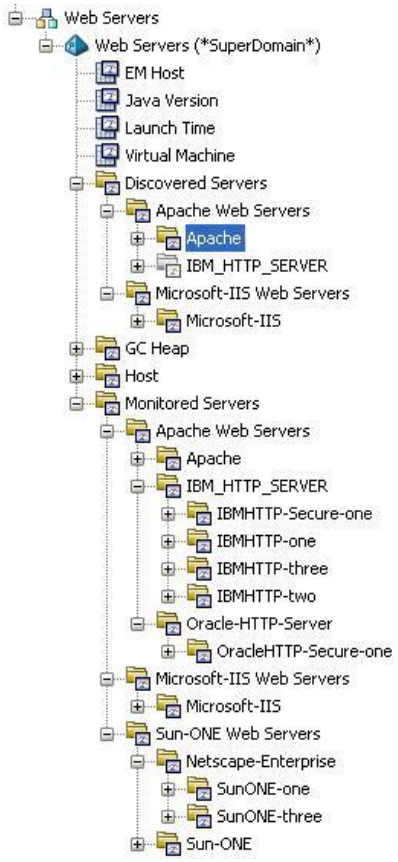
Using the CA APM for Web Servers with Introscope Workstation

To view web server metric information in Introscope:

1. Start the web server you want to monitor.
2. Start the CA APM for Web Servers.
3. Launch Enterprise Manager.
4. Launch and log into the Introscope Workstation.

Viewing web server metrics in the Introscope Investigator tree

Web server metric data is displayed in the Introscope Investigator tree under the Web Servers node, as shown in the following screenshot:



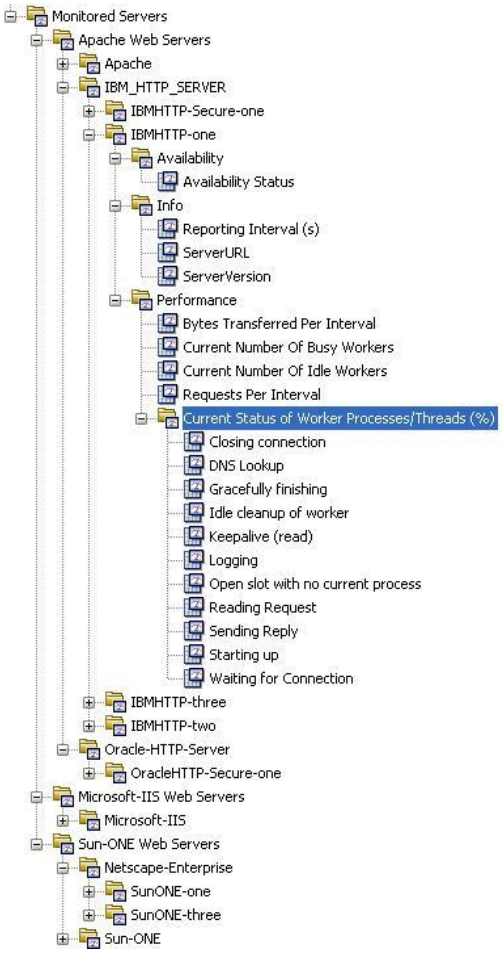
- To view web servers metrics, open an Introscope Investigator tree window.

Note: The metrics in the screenshot may differ from what you see, depending on which web servers are used in your environment.

You see two nodes under the Web Servers node:

- **Discovered Servers:** This node lists web servers (sorted by web server type and version) that were automatically discovered, but may not currently be monitored. Only IP Address and Port information are reported for Discovered Servers.
- **Monitored Servers:** This node lists web servers (sorted by web server type and version) currently being monitored. Additionally, Availability, Info, and Performance metrics are reported for Monitored Servers, as shown in the following screenshot.

Note: Name of the node may be different if the introscope.agent.agentname property in *WebServerAgent.profile* was modified.



Performance metrics are only reported if the web servers have been configured to publish their statistics. See Step 5: Configuring web servers to publish statistics (see page 28).

Details on exact metrics reported for each web server type is available.

More information:

CA APM for Web Servers metrics (see page 65)

Viewing the CA APM for Web Servers dashboards

The following sections show a subset of the dashboards available in the CA APM for Web Servers Management Module.

- To view dashboards, launch the Workstation, and open an Introscope console window.

  The extension provides several sample Dashboards for displaying a variety of web server performance metrics.

  Dashboards for the extension begin with "Web Servers" to distinguish them from Dashboards already installed in Introscope.

See the *CA APM Workstation Guide* for information on customizing Dashboards.

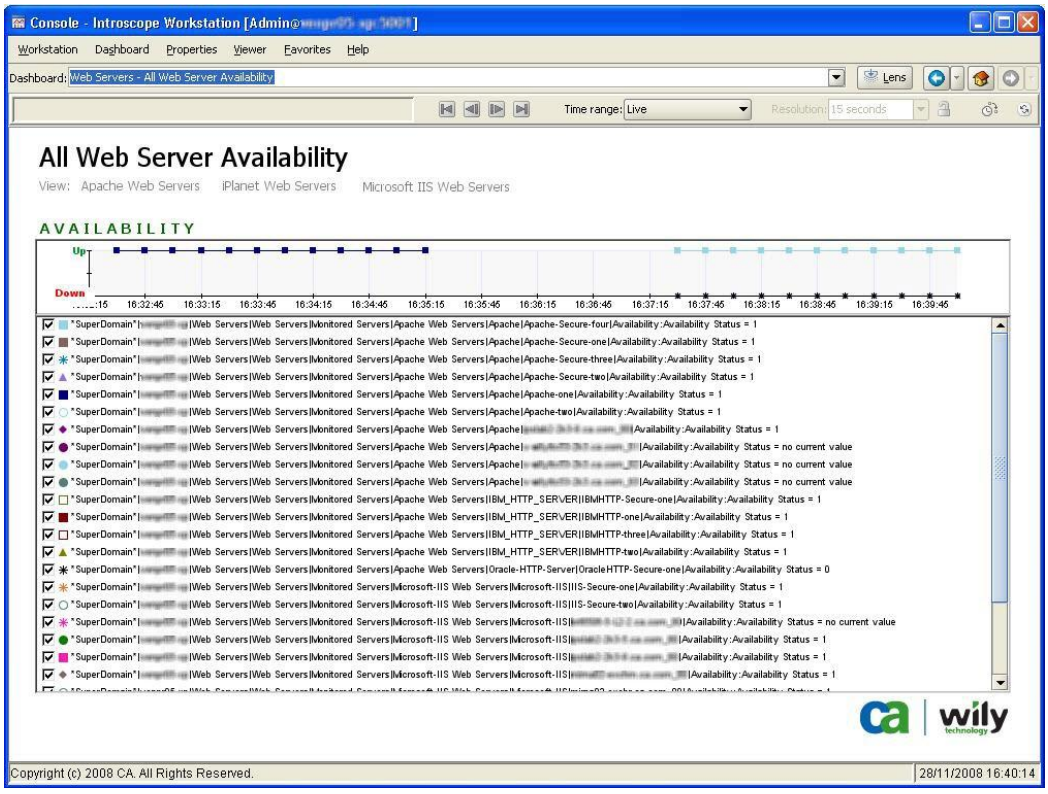
Web Servers Availability dashboard

When monitoring web servers, you may see the Web Servers Availability Dashboard. It shows you at a glance all the web servers currently being monitored by the CA APM for Web Servers.

The Availability graph shows whether a web server is up (value of 1) or down (value of 0).

From here you can drill down to Dashboards that contain metrics about specific web server types:

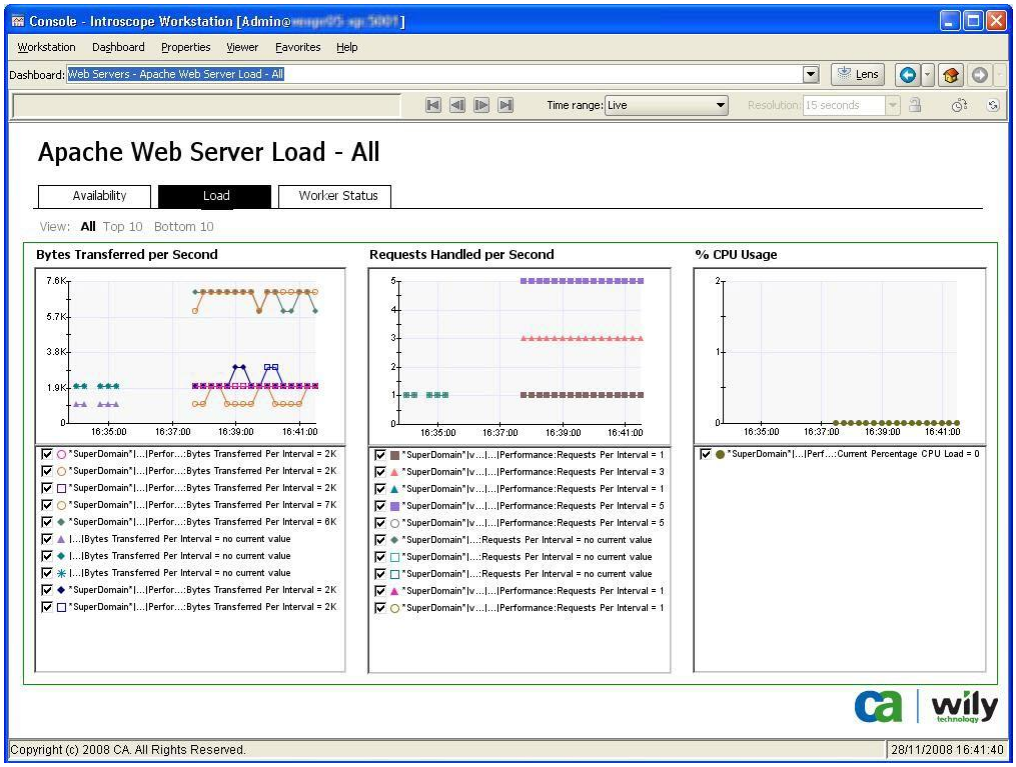
- Apache web servers
- Sun ONE (iPlanet) web servers
- Microsoft IIS web servers



Apache dashboards

There are seven Apache Dashboards:

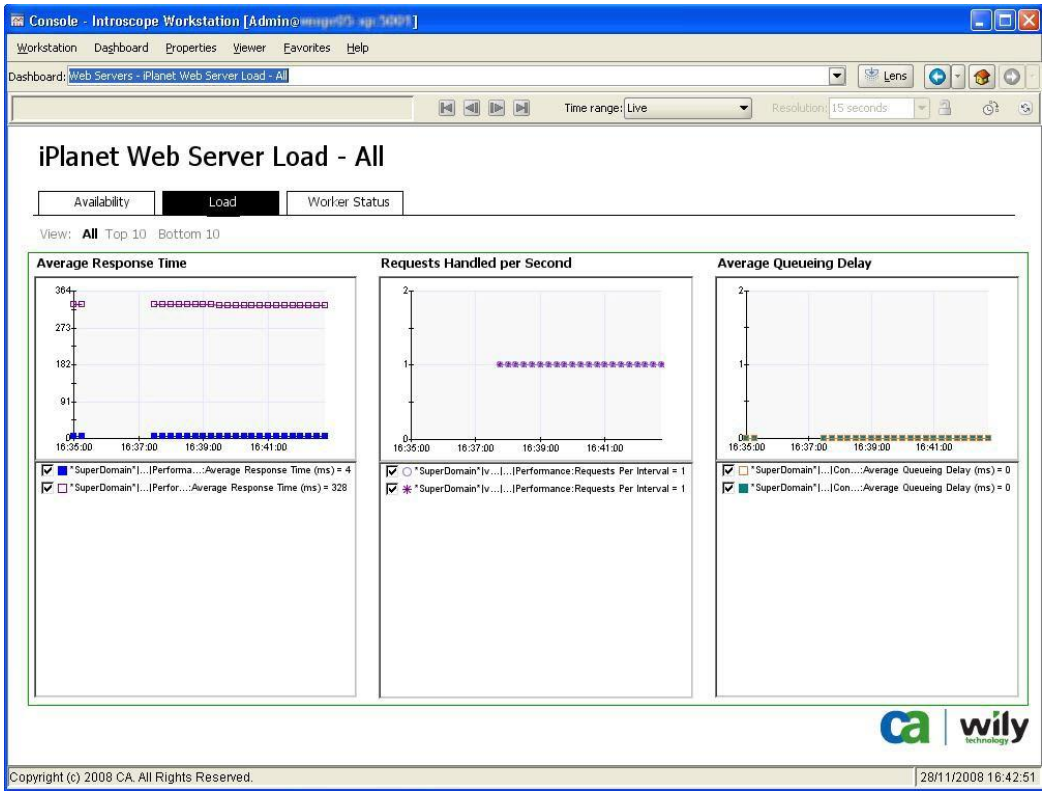
- Apache Web Server Availability
- Apache Web Server Load - All
- Apache Web Server Load - Bottom 10
- Apache Web Server Load - Top 10
- Apache Web Server Worker Status - All
- Apache Web Server Worker Status - Bottom 10
- Apache Web Server Worker Status - Top 10



Sun ONE (iPlanet) dashboard

There are seven Sun ONE (iPlanet) Dashboards:

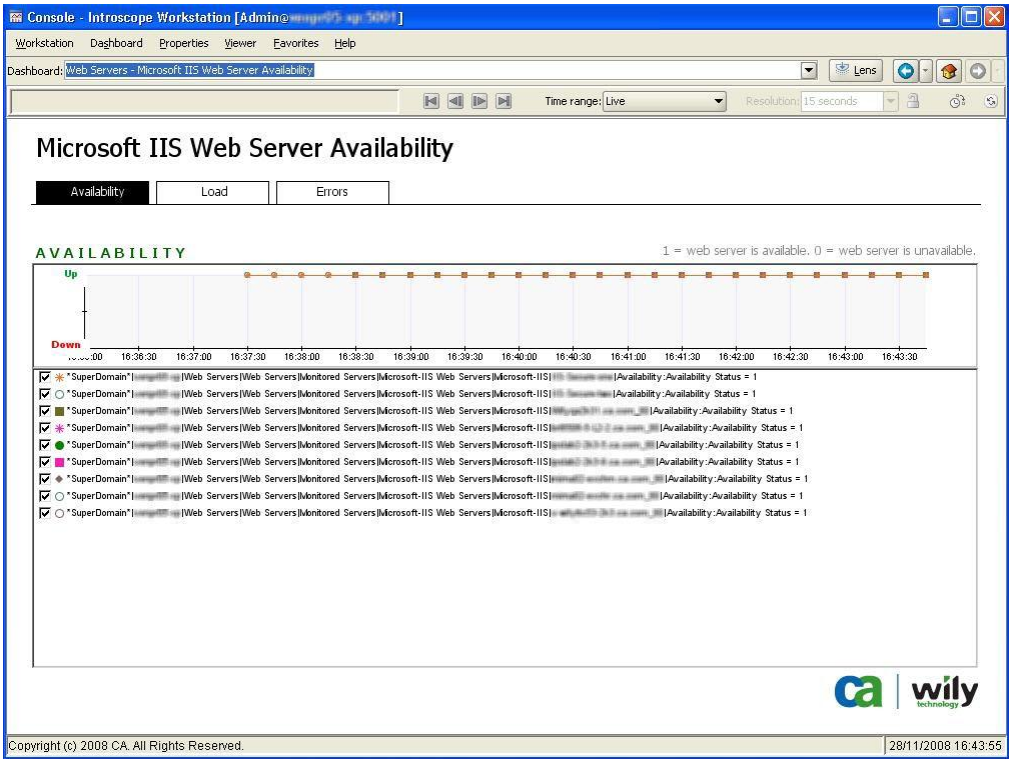
- iPlanet Web Server Availability
- iPlanet Web Server Load - All
- iPlanet Web Server Load - Bottom 10
- iPlanet Web Server Load - Top 10
- iPlanet Web Server Worker Status - All
- iPlanet Web Server Worker Status - Bottom 10
- iPlanet Web Server Worker Status - Top 10



Microsoft IIS Web Server dashboard

There are seven Microsoft IIS Dashboards:

- Microsoft IIS Web Server Availability
- Microsoft IIS Web Server Errors - All
- Microsoft IIS Web Server Errors- Bottom 10
- Microsoft IIS Web Server Errors - Top 10
- Microsoft IIS Web Server Load - All
- Microsoft IIS Web Server Load - Bottom 10



Appendix A: Metrics

This section describes the metrics reported by the CA APM for Web Servers.

This section contains the following topics:

CA APM for Web Servers metrics (see page 65)
Common metrics to all web servers (see page 65)
Apache, IBM HTTP Server, and Oracle HTTP Server metrics (see page 66)
Microsoft Internet Information Services (IIS) metrics (see page 69)
iPlanet (Sun ONE) Web Server metrics (see page 75)

CA APM for Web Servers metrics

All metrics appear in the Introscope Investigator tree under the Web Servers node.

There are two top-level nodes under the Web Servers node: Discovered Servers and Monitored Servers.

Common metrics to all web servers

Discovered Servers, Availability, and Info metrics are available for all monitored web servers.

Discovered Servers metrics

If a web server is discovered but not configured to be monitored, only the following metrics are available under the Discovered Servers node:

IP Address

The current IP address of the discovered web server.

Port

The port number that handles web service requests on the discovered web server.

Availability metrics

If a discovered web server is configured to be monitored, but not to publish its statistics, only Availability and Info metrics are published. The following metric is published for each monitored web server under the Availability node:

Availability Status

Specifies whether the web server is available. Values are up=1, and down=0.

Info metrics

If a discovered web server is configured to be monitored, but not to publish its statistics, only Availability and Info metrics are published. The following metrics are published for each monitored web server under the Info node:

ServerURL

URL of the web server.

ServerVersion

Web server type and version.

Reporting Interval (s)

Specifies how often the CA APM for Web Servers fetches statistics from the web server. The value is in seconds.

Mode

Specifies the mode that the CA APM for Web Servers uses to communicate with the web server using the HTTPS protocol. Mode can either be Permissive or Non-Permissive. Available only for web servers using HTTPS.

Apache, IBM HTTP Server, and Oracle HTTP Server metrics

The following metrics are published for Apache, IBM HTTP Server, and Oracle HTTP Server web servers when the web server is configured to publish metrics. For information about configuring a web server to publish metrics, see Publishing statistics on Apache and its derivatives (see page 29).

For more information about Apache-based metrics, see http://httpd.apache.org/docs/2.0/mod/mod_status.html.

Apache-based performance metrics

The following performance metrics are available for Apache, IBM HTTP Server, and Oracle HTTP Server web servers:

Bytes Transferred Per Interval

Total number of bytes served by the workers (server) per interval. Available only if ExtendedStatus is enabled.

Current Number of Busy Workers

The number of workers serving requests.

Current Number of Idle Workers

The number of idle workers.

Current Percentage CPU Load

The current percentage CPU used in total by all workers in the web server. Available only if ExtendedStatus is enabled. Available only for Apache servers on UNIX machines.

Requests Per Interval

Number of requests served by the workers (server) per interval. Available only if ExtendedStatus is enabled.

Current Status of Worker Processes/Threads (%)

The following metrics are available for Current Status of Worker Processes/Threads (%):

Closing connection

Percentage of workers closing connection already created.

DNS Lookup

Percentage of workers performing a DNS lookup for IP address to host name resolution.

Gracefully finishing

Percentage of workers doing a graceful finish operation before actually closing the connection.

Idle cleanup of worker

Percentage of workers doing an idle cleanup.

Keepalive (read)

Percentage of workers keeping some of the existing connections alive before timing out and closing it.

Logging

Percentage of workers involved in logging the activities to log files or custom log listeners.

Open slot with no current process

This percentage indicates the free slots for workers which can be filled up with a process due to incoming requests.

Reading Request

Percentage of workers reading a request in their process.

Sending Reply

Percentage of workers sending a reply in their process.

Starting up

Percentage of workers starting up in a new process to serve a request.

Waiting for Connection

Percentage of workers started and waiting for a connection so that it can begin processing requests.

Microsoft Internet Information Services (IIS) metrics

The following metrics are published for the Microsoft IIS web servers when the web server is configured to publish metrics. For information about configuring a web server to publish IIS metrics, see Publishing statistics for IIS 6.0 and 7.0 (see page 30).

For more information about Microsoft IIS metrics, see the following URLs:

- http://msdn.microsoft.com/library/default.asp?url=/library/en-us/wmisdk/wmi/win32_perfformatteddata_inetinfo_internetinformationservicesglobal.asp
- http://msdn.microsoft.com/library/default.asp?url=/library/en-us/wmisdk/wmi/win32_perfformatteddata_w3svc_webservice.asp

IIS performance metrics

Performance metrics for Microsoft IIS are organized into the following subnodes of metrics:

- User metrics
- I/O metrics
- Connections
- Requests
- Errors
- Caching
- Asynchronous I/O

User metrics

The following metrics for measuring Microsoft IIS performance are available under the User node:

AnonymousUsers Per Interval

Number of users making anonymous connections to the web server per interval.

CurrentAnonymousUsers

Number of users who currently have an anonymous connection with the web server.

NonAnonymousUsers

Number of users who currently have a non-anonymous connection with the web server.

LogonAttempts Per Interval

Number of logons being attempted to the web server per interval.

MaximumAnonymousUsers

Maximum number of users who established concurrent anonymous connections with the web server. This metric is counted after server start up.

MaximumNonAnonymousUsers

Maximum number of users who established concurrent non-anonymous connections with the web server. This metric is counted after server start up.

NonAnonymousUsers Per Interval

Number of users are making non-anonymous connections to the web server per interval.

I/O metrics

The following metrics for measuring Microsoft IIS performance are available under the I/O node:

BytesReceived Per Interval

Bytes received by the web server per interval.

BytesSent Per Interval

Bytes sent by the web server per interval.

BytesTransfered Per Interval

Sum of BytesSent Per Interval and BytesReceived Per Interval. This is the total number of bytes transferred by the web server per interval.

FilesTransfered Per Interval

File transferred per interval; that is, sent and received by the web server.

FilesReceived Per Interval

Files received by the web server per interval.

FilesSent Per Interval

Files sent by the web server per interval.

Connections

The following metrics for measuring Microsoft IIS performance are available under the Connections node:

ConnectionAttemptsallinstances Per Interval

Connection attempts made to the Web Server per interval.

CurrentConnections

Current number of connections established with the Web Server.

MaximumConnections

Maximum number of simultaneous connections established with the Web Server so far.

Requests

The following metrics for measuring Microsoft IIS performance are available under the Requests node:

CopyRequests Per Interval

Number of HTTP requests made per interval to the web server using the COPY method. COPY requests are used for copying files and directories.

CurrentISAPIExtensionRequests

Current number of ISAPI extension requests that are simultaneously being processed by the web server.

DeleteRequests Per Interval

Number of HTTP requests made per interval to the web server using the DELETE method. DELETE requests are generally used for file removal.

CGIRequests Per Interval

Number of CGI requests processed by the web server per interval.

CurrentCGIRequests

Current number of CGI requests that are simultaneously being processed by the web server.

GetRequests Per Interval

Number of HTTP requests made per interval to the web server using the GET method. GET requests are generally used for basic file retrievals or image maps, though they can be used with forms.

HeadRequests Per Interval

Number of HTTP requests made per interval using the HEAD method. HEAD requests generally indicate that clients are querying the state of documents they already have to see if they must be refreshed.

ISAPIExtensionRequests Per Interval

Number of ISAPI extension requests processed by the web server per interval.

LockRequests Per Interval

Number of HTTP requests made per interval to the web server using the LOCK method. LOCK requests are used to create lock for files.

MaximumCGIRequests

Maximum number of CGI requests simultaneously processed by the web server.

MaximumISAPIExtensionRequests

Maximum number of ISAPI extension requests simultaneously processed by the web server so far.

MkcolRequests Per Interval

Number of HTTP requests made per interval to the web server using the MKCOL method. MKCOL requests are used to create directories on the server.

MoveRequests Per Interval

Number of HTTP requests made per interval to the web server using the MOVE method. MOVE requests are used for moving files and directories.

OptionsRequests Per Interval

Number of HTTP requests made per interval using the OPTIONS method.

OtherRequestMethods Per Interval

Rate at which HTTP requests are made that do not use the OPTIONS, GET, HEAD, POST, PUT, DELETE, TRACE, MOVE, COPY, MKCOL, PROPFIND, PROPPATCH, MS-SEARCH, LOCK, or UNLOCK methods. These may include LINK or other methods supported by gateway applications.

PostRequests Per Interval

Number of HTTP requests made per interval to the web server using the POST method. POST requests are generally used for forms or gateway requests.

PropfindRequests Per Interval

Number of HTTP requests made per interval to the web server using the PROPFIND method. PROPFIND requests retrieve property values on files and directories.

ProppatchRequests Per Interval

Number of HTTP requests made per interval to the web server using the PROPPATCH method. PROPPATCH requests set property values on files and directories.

PutRequests Per Interval

Number of HTTP requests made per interval to the web server using the PUT method.

SearchRequests Per Interval

Number of HTTP requests made per interval to the web server using the MS-SEARCH method. MS-SEARCH requests query the server to find resources that match a set of client-provided conditions.

TraceRequests Per Interval

Number of HTTP requests made per interval to the web server using the TRACE method. TRACE requests allow the client to see what is being received at the end of the request chain and use the information for diagnostic purposes.

UnlockRequests Per Interval

Number of HTTP requests made per interval to the web server using the UNLOCK method. UNLOCK requests are used to remove locks from files.

Errors

The following metrics for measuring Microsoft IIS performance are available under the Errors node:

LockedErrors Per Interval

Number of errors reported per interval by the web server due to requests that cannot be satisfied by the server because the requested document was locked. These are generally reported as an HTTP 423 error code to the client.

NotFoundErrors Per Interval

Number of errors reported per interval by the web server due to requests that could not be satisfied by the server because the requested document could not be found. These errors are generally reported as an HTTP 404 error code to the client.

Caching

The following metrics for measuring Microsoft IIS performance are available under the BLOB Cache, File Cache, and URI Cache nodes.

BLOB Cache metrics

The following metrics for measuring Microsoft IIS performance are available under the BLOB Cache node:

BLOBCacheFlushes

BLOB cache flushes after server startup.

BLOBCacheHits

Total number of successful lookups in the BLOB cache.

BLOBCacheHits Percent

Ratio of BLOB cache hits to total cache requests.

BLOBCacheMisses

Total number of unsuccessful lookups in the BLOB cache.

CurrentBLOBsCached

BLOB information blocks currently in the cache for Internet and File Transfer Protocol (FTP) services.

File Cache metrics

The following metrics for measuring Microsoft IIS performance are available under the File Cache node:

CurrentFileCacheMemoryUsage

Current number of bytes used for file cache.

CurrentFilesCached

Current number of files whose content is in the cache for Internet and File Transfer Protocol (FTP) services.

FileCacheFlushes

File cache flushes after server startup.

FileCacheHits

Total number of successful lookups in the file cache.

FileCacheHitsPercent

Ratio of file cache hits to total cache requests.

FileCacheMisses

Total number of unsuccessful lookups in the file cache.

MaximumFileCacheMemoryUsage

Maximum number of bytes used for file cache.

URI Cache metrics

The following metrics for measuring Microsoft IIS performance are available under the URI Cache node:

CurrentURIsCached

URI information blocks currently in the cache for Internet and File Transfer Protocol (FTP) services.

URICacheFlushes

URI cache flushes after server startup.

URICacheHits

Total number of successful lookups in the URI cache.

URICacheHitsPercent

Ratio of URI cache hits to total cache requests.

URICacheMisses

Total number of unsuccessful lookups in the URI cache.

Asynchronous I/O

Asynchronous I/O metrics help measure IIS performance. They consist of these metrics:

CurrentBlockedAsyncIORequests

Current requests temporarily blocked due to bandwidth throttling settings.

MeasuredAsyncIOBandwidthUsage

Measured bandwidth of asynchronous I/O averaged over a minute.

iPlanet (Sun ONE) Web Server metrics

The following metrics are published for iPlanet 6.0, iPlanet 6.1, and Sun ONE 7.0 web servers when the web server is configured to publish metrics. For information about configuring a web server to publish metrics, see Publishing statistics for Sun ONE (see page 31).

For more information about iPlanet or Sun ONE metrics, see http://docs.sun.com/source/816-5690-10/perf6.htm#16363.

iPlanet performance metrics

The following metrics are available for iPlanet web servers under the Performance node:

Requests Per Interval

The total number of requests for the function per interval.

Average Response Time (ms)

The total time required by the server to process all the requests it has received so far in that interval.

Connection Queue

The following metrics are available for iPlanet web servers under the Connection Queue node:

Current Queue Length

The number of connections currently in the queue.

Peak Queue Length

The largest number of connections that have been in the queue simultaneously.

Maximum Allowed Queue Length

The maximum size of the connection queue.

Total Connections Queued

Total connections queued is the total number of times a connection has been queued. This includes newly accepted connections and connections from the keep-alive system.

Average Queueing Delay (ms)

Average queueing delay is the average amount of time a connection spends in the connection queue. This metric represents the delay between when a request connection is accepted by the server, and a request processing thread (also known as a session) begins servicing the request.

Keep Alive Info

The following metrics are available for iPlanet web servers under the Keep Alive Info node:

Current KeepAlive Connections

Number of connections in keep-alive mode.

Maximum Allowed KeepAlive Connections

Maximum number of connections allowed in keep-alive mode simultaneously.

KeepAlive Hits

The number of times a request was successfully received from a connection that had been kept alive.

KeepAlive Flushes

The number of times the server had to close a connection because the KeepAliveCount exceeded the MaxKeepAliveConnections.

KeepAlive Timeouts

Specifies the number of seconds the server will allow a client connection to remain open with no activity.

Session Creation Info

The following metrics are available for iPlanet web servers under the Session Creation Info node:

Active Sessions

The number of sessions (request processing threads) currently servicing requests.

Total Sessions Created

Total Sessions Created shows both the number of sessions that have been created and the maximum number of sessions allowed.

Maximum Allowed Sessions

The maximum number of sessions allowed.

Cache Info

The following metrics are available for iPlanet web servers under the Cache Info node:

Current Cache Entries

The number of current cache entries.

Maximum Allowed Cache Entries

The maximum number of cache entries.

Number of Cache Hits

Number of requests served from cache without actually processing the requests.

Number of Cache Lookups

Number of lookups into the cache by the web server for incoming requests before processing it.

Cache Hit Percentage

The number of file cache hits versus cache lookups in percentage.

Maximum Age

The maximum age displays the maximum age of a valid cache entry. This parameter controls how long cached information is used after a file has been cached.

Native Thread Pools

The following metrics are available for iPlanet web servers under the Native Thread Pool node:

Current Number of Idle Threads in Pool

The number of threads that are currently idle in the pool.

Peak Number of Threads in Pool

The peak is the highest number of number of threads ever in the pool.

Maximum Allowed Number of Threads in Pool

The maximum number of native threads allowed in the thread pool, and is determined by the setting of NativePoolMaxThreads.

Current Work Queue Length

The Work Queue Length is the current number of requests waiting for a native thread.

Peak Work Queue Length

Peak is the highest number of requests that were ever queued up simultaneously for the use of a native thread since the server was started. This value can be viewed as the maximum concurrency for requests requiring a native thread.

Maximum Allowed Work Queue Length

Maximum number of work queue length that can possibly be queued in the web server. Once it is full, no more requests can be added to the queue unless some requests are processed and removed from the queue.

Appendix B: CipherSuites supported by CA APM for Web Servers

This section contains the following topics:

CA APM for Web ServersCipherSuites (see page 79)

CA APM for Web ServersCipherSuites

The following list contains the CipherSuites that are supported by Java Secure Socket Extension (JSSE) 1.4.x onwards and the CA APM for Web Servers:

- *SSL_RSA_WITH_RC4_128_MD5*
- *SSL_RSA_WITH_RC4_128_SHA*
- *TLS_RSA_WITH_AES_128_CBC_SHA*
- *TLS_DHE_RSA_WITH_AES_128_CBC_SHA*
- *TLS_DHE_DSS_WITH_AES_128_CBC_SHA*
- *SSL_RSA_WITH_3DES_EDE_CBC_SHA*
- *SSL_DHE_RSA_WITH_3DES_EDE_CBC_SHA*
- *SSL_DHE_DSS_WITH_3DES_EDE_CBC_SHA*
- *SSL_RSA_WITH_DES_CBC_SHA*
- *SSL_DHE_RSA_WITH_DES_CBC_SHA*
- *SSL_DHE_DSS_WITH_DES_CBC_SHA*
- *SSL_RSA_EXPORT_WITH_RC4_40_MD5*
- *SSL_RSA_EXPORT_WITH_DES40_CBC_SHA*
- *SSL_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA*
- *SSL_DHE_DSS_EXPORT_WITH_DES40_CBC_SHA*
- *SSL_RSA_WITH_NULL_MD5*
- *SSL_RSA_WITH_NULL_SHA*
- *SSL_DH_anon_WITH_RC4_128_MD5*
- *TLS_DH_anon_WITH_AES_128_CBC_SHA*
- *SSL_DH_anon_WITH_3DES_EDE_CBC_SHA*

- *SSL_DH_anon_WITH_DES_CBC_SHA*
- *SSL_DH_anon_EXPORT_WITH_RC4_40_MD5*
- *SSL_DH_anon_EXPORT_WITH_DES40_CBC_SHA*
- *TLS_KRB5_WITH_RC4_128_SHA*
- *TLS_KRB5_WITH_RC4_128_MD5*
- *TLS_DH_anon_WITH_AES_256_CBC_SHA*
- *TLS_KRB5_WITH_3DES_EDE_CBC_SHA*
- *TLS_KRB5_WITH_3DES_EDE_CBC_MD5*
- *TLS_KRB5_WITH_DES_CBC_SHA*
- *TLS_KRB5_WITH_DES_CBC_MD5*
- *TLS_RSA_WITH_AES_256_CBC_SHA*
- *TLS_DHE_DSS_WITH_AES_256_CBC_SHA*
- *TLS_DHE_RSA_WITH_AES_256_CBC_SHA*
- *TLS_KRB5_EXPORT_WITH_RC4_40_SHA*
- *TLS_KRB5_EXPORT_WITH_RC4_40_MD5*
- *TLS_KRB5_EXPORT_WITH_DES_CBC_40_SHA*
- *TLS_KRB5_EXPORT_WITH_DES_CBC_40_MD5*

Appendix C: Sizing recommendations

This section describes the recommendations that are useful to monitor a large number of web servers with CA APM for Web Servers.

This section contains the following topics:

Metric Limits (see page 81)
Heap Sizing (see page 83)

Metric Limits

The following table gives the maximum number of metrics reported for a web server by CA APM for Web Servers.

Web Server	Number of Metrics Reported
Apache/IBM HTTP Server (IHS)/Oracle HTTP Server (OHS)	19
Microsoft IIS	63
Sun ONE (iPlanet)	31

Note: If a web server is monitored over HTTPS, an additional HTTP monitoring metric is reported under Info|Mode node. See Common metrics to all web servers (see page 65) for details. If Apache, IBM HTTP Server, or Oracle HTTP Server is being monitored and is installed on UNIX or Linux, an additional metric under Performance|Current Percentage CPU Load node is reported for each web server. See Apache/IHS/OHS metrics (see page 66) for details.

To compute the total number of metrics that are reported by CA APM for Web Servers to the Enterprise Manager, use the following formula:

$$metric\ count = 19a + 20b + 20c + 21d + 63e + 64f + 31g + 32h$$

where

- *a* is the number of Apache based web servers monitored in HTTP mode
- *b* is the number of Apache based web servers monitored in HTTPS mode
- *c* is number of Apache based web servers monitored in HTTP mode
- *d* is the number of Apache based web servers monitored in HTTPS mode
- *e* is the number of IIS web servers monitored in HTTP mode
- *f* is the number of IIS web servers monitored in HTTPS mode

- *g* is the number of iPlanet (Sun ONE) web servers monitored in HTTP mode
- *h* is the number of iPlanet (Sun ONE) web servers monitored in HTTPS mode

Note: In the formula, Apache based web server represents Apache, IBM HTTP Server, or Oracle HTTP Server installed on Windows based platform.

To report all of the metrics for each of the monitored web servers, you must configure the following properties in *apm-events-thresholds-config.xml* and *WebServerAgent.profile* files while configuring the Enterprise Manager and the CA APM for Web Servers:

- In the *apm-events-thresholds-config.xml* file, located in the <EM_Home>/config director, specify values for the following properties:
  - *introscope.enterprisemanager.agent.metrics.limit*
  - *introscope.enterprisemanager.metrics.live.limit*

  Note: For more information about these properties, see the *CA APM Configuration and Administration Guide*.
- In *WebServerAgent.profile* file that is shipped with the CA APM for Web Servers, specify value for the following property:

  introscope.agent.metricClamp

  Note: For more information about this property, see the *CA APM Java Agent Implementation Guide*.

Important! The values for the properties must be specified as integers and must be greater than the value of *metric count* in the above-mentioned formula.

Heap Sizing

By default the maximum Java heap size is specified as 512MB for CA APM for Web Servers. If this heap size is not sufficient for the number of web servers that have been configured to be monitored by CA APM for Web Servers, perform the following steps to adjust the Java heap size.

To adjust the Java heap size:

1. If CA APM for Web Servers is installed on Windows, open the *.\jsw-3.2.3\conf\wrapper.conf* file and edit the following properties:

   a. To set the minimum heap size, uncomment the property
   wrapper.java.initmemory=3

   and specify the required value in MB for maximum heap size instead of 3.

   b. To change the maximum heap size, edit the property

   wrapper.java.maxmemory=512

   and specify the required value in MB for maximum heap size instead of 512.

2. If CA APM for Web Servers is installed on UNIX or Linux, open the *WebServerMonitor.sh* and edit the following properties:

   a. To change the maximum heap size, locate the line containing
   -Xmx512m

   and specify the required value in MB for maximum heap size instead of 512.

   b. To change the minimum heap size, add the following argument to the same line:
   -Xms(mb)m

   where (mb) is the required minimum heap size value in MB.

   For example, the default *WebServerMonitor.sh* has the following line:

   ```
   nohup java -cp
   ./lib/WebServerAgent.jar:./lib/PPWebServers.jar:./lib/commons-logging-1.1
   .jar:./lib/commons-codec-1.3.jar:./lib/jline-0.9.9.jar -Xmx512m
   -Dcom.wily.introscope.agentProfile=./config/WebServerAgent.profile
   com.wily.webservermonitor.Main  > /dev/null 2>&1 &
   ```

   To change the minimum and maximum Java heap size to 10 MB and 256 MB, edit the line as follows:

   ```
   nohup java -cp
   ./lib/WebServerAgent.jar:./lib/PPWebServers.jar:./lib/commons-logging-1.1
   .jar:./lib/commons-codec-1.3.jar:./lib/jline-0.9.9.jar –Xms10m  -Xmx256m
   -Dcom.wily.introscope.agentProfile=./config/WebServerAgent.profile
   com.wily.webservermonitor.Main  > /dev/null 2>&1 &
   ```

3. After making the changes to *WSPPService.conf* or *WebServerMonitor.sh* file, save the file and restart the CA APM for Web Servers.

Appendix D: Frequently Asked Questions

This appendix contains frequently asked questions regarding the CA APM for Web Servers.

This section contains the following topics:

Upgrading the CA APM for Web Servers (see page 85)
Monitoring web servers (see page 85)
Discovery of web servers (see page 88)
Improved web server support (see page 89)
AgentConfigTool utility (see page 90)
General (see page 91)

Upgrading the CA APM for Web Servers

Q. Why can't I update the old version of the WebServerConfig.xml file directly using the UpdateMonitorConfigFile utility?

A. The *WebServerConfig.xml* file has comments and instructions about the attributes. So for your future reference, we recommend copying the web server definitions from the old to new file and then updating it. This would ensure that you don't lose any comments.

Q. Can I use the UpdateMonitorConfigFile utility to upgrade the DiscoveryConfig.xml?

A. No. *UpdateMonitorConfigFile* utility can only be used for upgrading *WebServerConfig.xml* file. *DiscoveryConfig.xml* file has comparatively less content and thus can be upgraded manually.

Monitoring web servers

Q. For monitoring and getting performance metrics of a new web server based on standard base types of Sun ONE, Apache and Microsoft IIS, is there any requirement?

A. Yes. For Apache based web server the *mod_status* module must be available. Sun ONE servers must have *service-dump* function and WMI classes must be available on IIS web server machine.

Q. I am trying to monitor a web server configured to communicate over HTTPS. For this, I modified the ServerURL attribute in WebServerConfig.xml to have https instead of http. However, I don't see the server getting monitored. What could be wrong?

A. When monitoring a web server over HTTPS, CA APM for Web Serversdefaults to the non-permissive mode. Additionally, it uses SSL v3.0 protocol by default unless specified otherwise. In case you want to monitor the web server in non-permissive mode, you need to import the web server certificate in a trust store file and give that as an input to CA APM for Web Servers. In case you don't want to provide the web server certificate, you can opt for the permissive mode by setting the *Mode* attribute in the *WebServerConfig.xml* to *Permissive*.

Q. I have defined some web servers in the WebServerConfig.xml file with non-permissive mode. However, none of the web servers are getting monitored. What could be wrong?

A. Ensure that you have imported all the web server certificates in a truststore file and given that as an input to CA APM for Web Servers. This can be done by setting the truststore settings using *AgentConfigTool* utility.

Q. I've deployed the CA APM for Web Servers and configured to monitor a web server, but the Availability metrics show the status as zero in the Investigator tree even though the web server is up and running. What could be wrong?

A. This indicates that the CA APM for Web Servers is unable to establish a connection with the web server. Ensure that the port on which the web server is running is not blocked. Also in case the monitoring is happening over HTTPS, the web server should be configured to communicate over SSL v3.0 or TLS v1.0 protocols.

Q. Are all formats for Public Key Certificate supported by the CA APM for Web Servers?

A. No, only X.509 Public Key Infrastructure Certificate formats are supported by the CA APM for Web Servers.

Q. How can I know whether WMI classes are available in the IIS web server machine or not?

A. Copy the IIS files to the web server machine and extract it. Modify the *VBScript.bat* manually to provide valid locations of *PublishIISStats.vbs* and stats page. Open a command prompt and navigate to the directory where the IIS archive has been extracted. Now from command prompt run *VBScript.bat*. The batch file should not exit with an error. If it exits with an error, something like *<Location of PublishIISStats.vbs>(51, 2) (null): 0x80041010* then WMI classes are not available in the machine and we will not be able to get any performance metrics for that server.

Q. I have a new web server that is not yet available for access to anyone but the CA APM for Web Servers agent. I enabled performance metrics and for some metrics like Requests per Interval, NotFoundErrors etc., I see some constant values. Is this a normal behavior?

A. Yes, it is absolutely normal. In order to get the performance metrics from a web server we establish a connection with the server at a defined frequency. This results in some of those metrics with values.

Q. Can I specify the metrics to be monitored for web servers?

A. No, you cannot. We only report certain useful metrics with no flexibility of explicitly mentioning metric names.

Q. I have an IIS web server with Windows Integrated Authentication turned on. Can the CA APM for Web Servers monitor this server?

A. No, the CA APM for Web Servers cannot monitor an authenticated web server. The CA APM for Web Servers doesn't provide an option to specify username and password to connect to the web server. In case these web servers need to be monitored, the stats page can be selectively given anonymous access to the CA APM for Web Servers. To do this, right click on the IISPERFSTATS virtual directory and go to Properties > Directory Security. Thereafter go to Authentication and access control and edit the configuration to permit anonymous access. Optionally, you can also go to IP address and domain name restrictions and configure the server to permit the client IP only to access this page. Client IP is the IP of the machine on which the CA APM for Web Servers is installed.

Q. My IIS web server is running over PCT 1.0 protocol and I am trying to monitor it with the CA APM for Web Servers and it is showing Availability as zero. What could be wrong?

A. The CA APM for Web Servers supports only SSL v3.0 and TLS v1.0 protocols only. So you will not be able to monitor the IIS web server running over PCT 1.0 or SSL v2.0 protocol.

Q. Can the CA APM for Web Servers monitor a web server fronted by a proxy server?

A. No. This is not supported.

Q. Do I need to restart the CA APM for Web Servers after I change the Protocol of a web server in WebServerConfig.xml?

A. No. *Protocol*, *Mode*, *DisplayName*, *Server-URL*, and *RefreshFrequencyInSeconds* attributes are dynamic. They don't require a restart of the CA APM for Web Servers. These values are picked by the CA APM for Web Servers in the next monitoring cycle. The monitoring cycle runs every minute.

Q. I see a metric named Mode under Info node in Investigator. What does this metric signify?

A. *Mode* metric is seen only for web servers running over HTTPS. This metric tells us the mode in which a particular web server is being monitored by CA APM for Web Servers. Possible values of the Mode metric are Permissive and Non-Permissive. The Permissive mode doesn't require any web server certificate while the Non-Permissive mode needs it.

Q. With the CA APM for Web Servers v1.x I see the Apache web server under its version node in Investigator tree. But in this release I see it under "Apache" node. Is this an expected behavior?

A. Yes. With this release you will see the monitored web servers under their parent name. For example, IBM HTTP Server, Oracle HTTP Server, and Apache web servers will be shown under "Apache Web Servers" node since they are derived from Apache. Similarly all versions of IIS web servers will be shown under "Microsoft-IIS Web Servers" and Sun ONE web servers under "SUN ONE Web Servers" node.

Q. I have specified the RefreshFrequencyInSeconds attribute in the WebServerConfig.xml but have not specified its value. Why am I seeing a parsing error "Error parsing configuration file. Will retry after 1 minute(s)."?

A. If you have given *RefreshFrequencyInSeconds* in *WebServerConfig.xml* as *RefreshFrequencyInSeconds=* and not specified any value, this parsing error occurs. Specify a value for the attribute or remove the attribute from the file. The default value of 15 seconds will be taken for *RefreshFrequencyInSeconds* if the attribute is not included.

Discovery of web servers

Q. Is discovery valid for an IPv6 subnet?

A. Yes, it is valid. Remember that larger the number of hosts to scan in a subnet, larger the time it takes for the discovery to complete. We recommend a range of IPv6 addresses with considerably lesser number of hosts to scan than a single IPv6 subnet.

Q. Can I increase the value of the <Concurrency> attribute in DiscoveryConfig.xml?

A. Yes, you can. This concurrency defines the number of threads for each subnet configured and increasing it will increase the total number of threads running for this process which will in turn consume more CPU cycles. It's recommended not to alter the default value for this attribute.

Q. I have a subnet where there are some web servers configured over HTTP and some over HTTPS. I would like to discover both the class of web servers. How do I specify this in the DiscoveryConfig.xml?

A. Apart from providing the subnet details, such as range, you need to specify the ports on which the different web servers are listening for HTTP and HTTPS connections. Identify the HTTP and HTTPS ports and segregate them. The HTTP ports can be directly specified. For the HTTPS ports, you have to specify the *Protocol* attribute. This lets the CA APM for Web Servers know that these ports are listening for HTTPS connections. Additionally the Protocol attribute's value specifies the protocol (SSL or TLS) over which CA APM for Web Servers should try establishing a connection with the web server. This is illustrated in the example. Discovery at port 80 would occur over HTTP protocol while at 443 it would occur over HTTPS. This is because of specification of the Protocol attribute.

```
// HTTP Port
<Port Number="80" Type="TCP" >
        <FingerPrintMatcher>Apache</FingerPrintMatcher>
        <FingerPrintMatcher>Apache:IBM_HTTP_SERVER</FingerPrintMatcher>
        <FingerPrintMatcher>Apache:Oracle-HTTP-Server
    </FingerPrintMatcher>
        <FingerPrintMatcher>Microsoft-IIS</FingerPrintMatcher>
        <FingerPrintMatcher>Sun-ONE</FingerPrintMatcher>
        <FingerPrintMatcher>Sun-ONE:Netscape-Enterprise
    </FingerPrintMatcher>
    </Port>
// HTTPS Port
    <Port Number="443" Type="TCP" Protocol="SSL" Mode="Permissive">
        <FingerPrintMatcher>Apache</FingerPrintMatcher>
        <FingerPrintMatcher>Apache:IBM_HTTP_SERVER</FingerPrintMatcher>
        <FingerPrintMatcher>Apache:Oracle-HTTP-Server
    </FingerPrintMatcher>
        <FingerPrintMatcher>Microsoft-IIS</FingerPrintMatcher>
        <FingerPrintMatcher>Sun-ONE</FingerPrintMatcher>
        <FingerPrintMatcher>Sun-ONE:Netscape-Enterprise
    </FingerPrintMatcher>
    </Port>
```

Improved web server support

Q. Should I include a base and variant necessarily for a new web server based on Apache?

A. Yes you must. The base type is used to identify the family of the web server, such as, Apache, Sun ONE, or IIS, and the variant type to discover it. For example, if you have a look at the *DiscoveryConfig.xml*, the IBM HTTP Server is mentioned as Apache:IBM_HTTP_SERVER. Here Apache is the base type and IBM_HTTP_SERVER is the variant type.

Q. What would happen if I put the correct variant with a wrong base type name?

A. You will be able to discover the web server, but you might not be able to get the performance metrics. Also you might end up getting the variant node under a different family in the Introscope Investigator. So please ensure that the variant is really based on the base type before giving it in the configuration files. For example, Oracle HTTP Server is based on Apache server. So it should be given as *Apache:Oracle-HTTP-Server* and not *Microsoft-IIS:Oracle-HTTP-Server*.

Q. How should I find the variant name of a new Apache based web server that I want to monitor?

A. The CA APM for Web Servers archive contains a tool called *ServerVersionFinder* that can be used to find the Server Header of an HTTP or HTTPS URL. See To find the Server Header of a given HTTP or HTTPS Server: on page 45 for details.

Q. Is there any restriction while specifying the values of all the attributes/tags in the configuration files, that is, WebServerConfig.xml and DiscoveryConfig.xml?

A. Yes. You cannot use XML special characters like ", ', <, >, and & directly as values or inputs in the *WebServerConfig.xml* and *DiscoveryConfig.xml* configuration files. Instead of that use the XML equivalents, that is, ", ', <, >, and & For example, if your *MetricsURL* attribute has to hold a value "perf&data", you can mention it like "perf&data" in the *WebServerConfig.xml* file.

Q. Is it necessary to give a multiplier or a divisor in ApacheCustomMetrics.xml file along with a custom metric name?

A. No. If nothing is mentioned, default value of 1 is taken for both the multiplier and divisor.

AgentConfigTool utility

Q. I understand that AgentConfigTool.bat puts the entries into AgentConfig.properties file. However, can I still manually edit the truststore settings in the file?

A. No. *AgentConfigTool.bat* stores the TrustStore password in *AgentConfig.properties* file in encrypted format. Changing it manually will result in wrong password.

Q. I have changed the truststore settings using AgentConfigTool.bat but new values are not being taken by the CA APM for Web Servers. Why could this be happening?

A. You need to restart your CA APM for Web Servers after changing truststore settings to come into effect.

General

Q. Does the CA APM for Web Servers ship a private JRE? If not, how do I identify the version of JRE that CA APM for Web Servers currently uses?

A. The CA APM for Web Servers does not ship a private JRE. CA APM for Web Servers takes the JRE from the PATH variable. Ensure that the PATH environment variable is updated with a supported JRE (see page 21).

Q. Why does the error "Can't load IA 32-bit .dll on a IA 64-bit platform" appear when I run the AgentConfigTool.bat file?

A. This error occurs when you have configured the CA APM for Web Servers to work with a 64-bit JRE. The product is supported (see page 21) on a 64-bit platform when you use a 32-bit JRE.

Q. Can I set up an Alert based on the Availability metric?

A. Yes. Alerts can be set on all the metrics reported by the CA APM for Web Servers.

Q. Can I use the CA APM for Web Servers agent to communicate to Enterprise Manager over HTTPS?

A. Yes, the CA APM for Web Servers agent can connect to Enterprise Manager over HTTP or HTTPS and also through a forward proxy server. You can also configure it for agent-side metric aging and metric clamping. You can find all the related properties in WebServerAgent.profile file.

Q. Why am I unable to connect CA APM for Web Servers to Introscope 7.2 Enterprise Manager?

A. CA APM for Web Servers 9.1.1 only supports Introscope 9.0 at a minimum, so it cannot connect to prior versions of Enterprise Manager. The following error may appear:

[IntroscopeAgent.OutgoingConnection] Client connection attempt timed out after 120000 milliseconds …

Q. Can the CA APM for Web Servers help me identify load on a web server?

A. Yes. The CA APM for Web Servers dashboards help you identify the heavily loaded web servers.

Q. Does CA APM for Web Servers work in an IPv6 environment?

A. IPv6 support on the agent is dependent on IPv6 support in the environment (JVM, operating system, hardware stack, web server) in which the agent is running.

Q. How do I enable logging for CA APM for Web Servers?

A. To enable VERBOSE mode logging, modify the WebServerAgent.profile file as follows:

```
log4j.logger.IntroscopeAgent=VERBOSE#com.wily.util.feedback.Log4JSeverityLevel,
console, logfile
log4j.logger.WebServerMonitor=VERBOSE#com.wily.util.feedback.Log4JSeverityLevel,
console, logfile
log4j.logger.AutoDiscoveryEngine=VERBOSE#com.wily.util.feedback.Log4JSeverityLeve
l, console, logfile
```

To enable DEBUG mode logging, modify the WebServerAgent.profile file as follows:

```
log4j.logger.IntroscopeAgent=DEBUG, console, logfile
log4j.logger.WebServerMonitor=DEBUG, console, logfile
log4j.logger.AutoDiscoveryEngine=DEBUG, console, logfile
```

For assistance, contact CA Support at http://ca.com/support.

Appendix E: IPv6 support

CA APM for Web Servers is IPv6 certified.

This section contains the following topics:

Connecting to Enterprise Manager on IPv6 (see page 93)

Connecting to Enterprise Manager on IPv6

To enable display of the IPv6 IP address in the Investigator in a pure IPv6 Java environment, you must configure the agent *java.net.preferIPv6Addresses* property.

To configure the agent java.net.preferIPv6Addresses property:

- **On Windows:** Update the *java.net.preferIPv6Addresses* property in the Java Additional Parameters section of the *wrapper.conf* file in the *<PPWebServersHome>/jsw-3.2.3/conf* directory as follows:
  ```
  wrapper.java.additional.1=
  -Dcom.wily.introscope.agentProfile=../../config/WebServerAgent.profile
  -Djava.net.preferIPv6Addresses=true
  ```
- **On UNIX:** Update the *java.net.preferIPv6Addresses* property in the startWSAgent function present in the *<PPWebServersHome>\WebServerMonitor.sh* shell script as follows:
  ```
  nohup java -cp
  ./lib/WebServerAgent.jar:./lib/PPWebServers.jar:./lib/commons-logging-1.1.jar
  :./lib/commons-codec-1.3.jar:./lib/jline-0.9.9.jar -Xmx512m
  -Djava.net.preferIPv6Addresses=true
  -Dcom.wily.introscope.agentProfile=./config/WebServerAgent.profile
  com.wily.webservermonitor.Main  > /dev/null 2>&1 &
  ```

Note: When you set *-Djava.net.preferIPv6Addresses=true*, the Investigator displays the full IPv6 IP address under **SuperDomain* |<AgentName> | Web Servers| Web Servers (*SuperDomain*)| Host | IP Address*. However, if the IPv6 address is not mentioned in the hosts file of the machine on which the agent is running, the Investigator displays 0:0:0:0:0:0:0:1.

Index

A

agent files
  UNIX • 40
  Windows • 25
AgentConfig.properties
  AgentConfigTool.sh • 41
  auto discovery • 32
  configuring • 27
  location • 25
Apache web servers
  configuring statistics • 29
  custom metric config file path • 41
  customizing metrics • 37
  dashboards • 62
  metrics • 66
  support for • 51
auto-discovery
  web servers • 32

C

CipherSuites • 79

D

dashboards
  Apache • 62
  Sun ONE • 63
  Web Servers Availability • 61
DiscoveryConfig.xml • 32

E

Enterprise Manager
  installing, UNIX • 39
  installing, Windows • 23
  Management Module • 36

F

functionality • 18

H

HTTPS
  configuring • 49
  finding the Server Header • 51
  support for • 49

I

IIS
  dashboards • 64
  metrics • 69
  publishing statistics • 30
  support for • 51
installing
  CA APM for Web Servers, Windows • 24
  configuring Agent profile, UNIX • 40
  configuring AgentConfig.properties • 41
  configuring per-interval metrics • 55
  defining web servers to monitor • 31
  Management Module • 36
  manual configuration for monitoring • 35
  publishing web server statistics, UNIX • 28
  requirements • 21
  upgrading from 1.0 • 46
  WebServerAgent profile • 24
  Windows files • 25
  Windows, overview • 23

M

Management Module
  installing • 36
  installing, Windows • 24
metrics
  Apache • 66
  CipherSuites • 79
  customizing Apache • 37
  Discovered Servers • 65
  IHS • 66
  Info • 66
  Microsoft IIS • 69
  per-interval configuration • 55
  Sun ONE • 75
  viewing in Introscope • 57
  viewing in Introscope Investigator • 58
monitoring
  configuring HTTPS • 49
  HTTPS protocol • 49
  manual configuration • 35
  web servers • 31

O

Oracle HTTP Server
    support for • 51
overview • 17

P

PPWebServersHome • 21

S

service
    Windows • 27
SSL • 49
standalone agent installer • 24
starting the CA APM for Web Servers
    UNIX • 43
    Windows • 37
statistics
    configuring Apache • 29
    configuring published HTML file • 56
    IIS • 30
    publishing, UNIX • 28
    Sun ONE • 31
stopping the CA APM for Web Servers
    UNIX • 44
    Windows • 38
Sun JRE • 21
Sun ONE
    dashboards • 63
    metrics • 75
    publishing statistics • 31
    support for • 51

U

UNIX
    CA APM for Web Servers agent files • 40
    Enterprise Manager installation • 39
    installing, overview • 39
    restarting the CA APM for Web Servers • 44
    running the CA APM for Web Servers • 43
    stopping CA APM for Web Servers • 44
upgrading
    from 1.0 • 46

V

viewing web server metrics • 57

W

web servers
    viewing metrics • 57
WebServerAgent profile • 24
Windows
    deregistering the service • 38
    installation overview • 23
    Windows, registering the extension as a service • 27