CA Application Performance Management

Integration for CA Infrastructure Management Guide (2.0.00)

Release 9.2

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 Web Access Manager (CA APM for CA SiteMinder Web Access Manager)
- 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)
- 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 that you need for your Home Office, Small Business, and Enterprise CA Technologies products. At http://ca.com/support, you can access the following resources:

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

Providing Feedback About Product Documentation

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

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

CA APM product names that appear in this guide have been updated to reflect the current naming conventions.

- CA NetQoS Performance Center is now CA Performance Center.
- CA Application Delivery Analysis Management Console is now CA Application Delivery Analysis Manager.
- Network Aware Application Triage solution is now Unified End User Experience Monitoring solution.
- Multi-Port Collector is now Multi-Port Monitor.

CA Technologies Product References

CA APM documentation includes information for CA APM, CA Introscope, 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, 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 and for CA CEM. CA Introscope and CA CEM properties are documented in the appendix.
- *CA APM Security Guide* — Choosing and configuring CA APM, CA Introscope, 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. CA APM documentation is also pertinent for CA Introscope.

- *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 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 dashboards, Investigator tree and application triage map, Transaction Tracer, and reporting. Includes CA Introscope metrics overview and descriptions.
- *CA APM WebView User Guide* — Using WebView to view CA Introscope 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 Web Access Manager Guide* — Installing, configuring, and using CA APM for CA SiteMinder Web Access Manager.
- *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 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.
- *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. Lets you monitor the health metrics of critical mainframe components.
- *CA Introscope SAP NetWeaver Conversion Guide* — Using CA APM for SAP NetWeaver.
- *CA Introscope WebView User Guide for SAP* — Using WebView for SAP.

CA Technologies Product References

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 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: Introduction

This section contains the following topics:

Unified End-User Experience Monitoring

Unified End-User Experience Monitoring is the integration between CA APM and CA Infrastructure Management. The integration provides visibility into application level data that is related to application usage for an end user. Additionally, the integration utilizes the Multi-Port Monitor, with CA APM Transaction Impact Manager (TIM) installed, to monitor your application and network infrastructure. With TIM installed on Multi-Port Monitor, the appliance is often referred to as a converged appliance.

This integration lets you analyze data and triage from the following perspectives:

CA CEM Console

Use the application and infrastructure metrics to identify a potential performance issue and navigate directly to Multi-Port Monitor for further investigation.

CA Introscope Workstation

Investigate infrastructure performance issues using server and client subnet metrics, and then navigate directly to CA Performance Center for more in-depth analysis. You can also use the infrastructure metrics to create custom dashboards.

CA Performance Center

Analyze HTTP metrics down to the defect level and navigate directly to the specific client subnet and server for further investigation. CA APM integrates by implementing a set of web services and connecting to the Application Performance Management data source.

Multi-Port Monitor

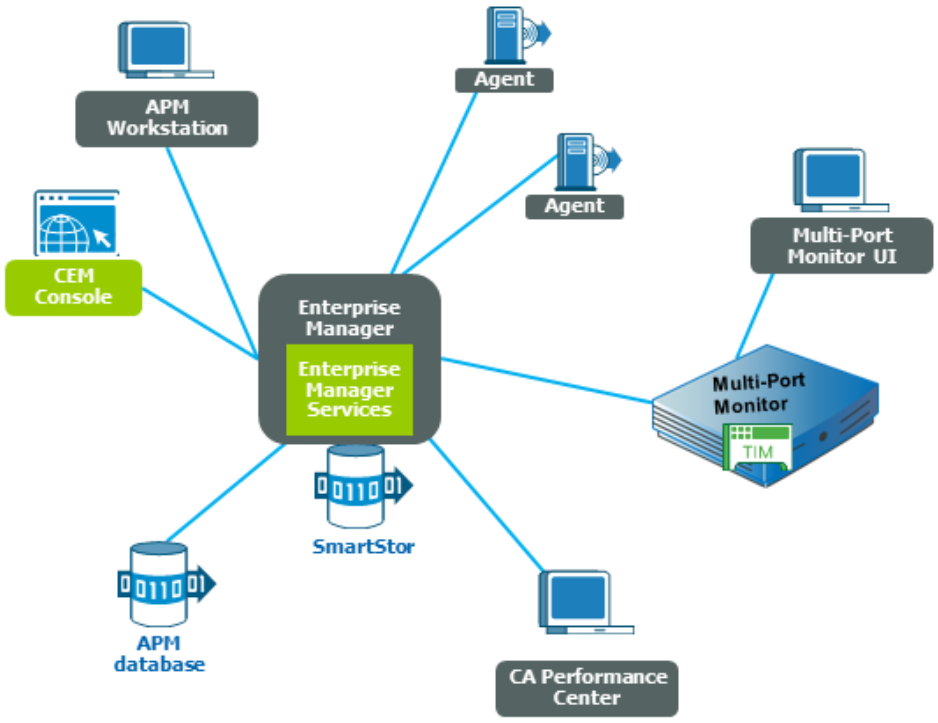
Analyze session level data and export reports to see and further analyze packet details.

Deployment Architecture

The Unified End-User Experience Monitoring solution provides many deployment options, depending on the size and complexity of your network. This section outlines two possible scenarios.

In smaller environments where a single Multi-Port Monitor is sufficient, your deployment architecture may look similar to the following diagram.

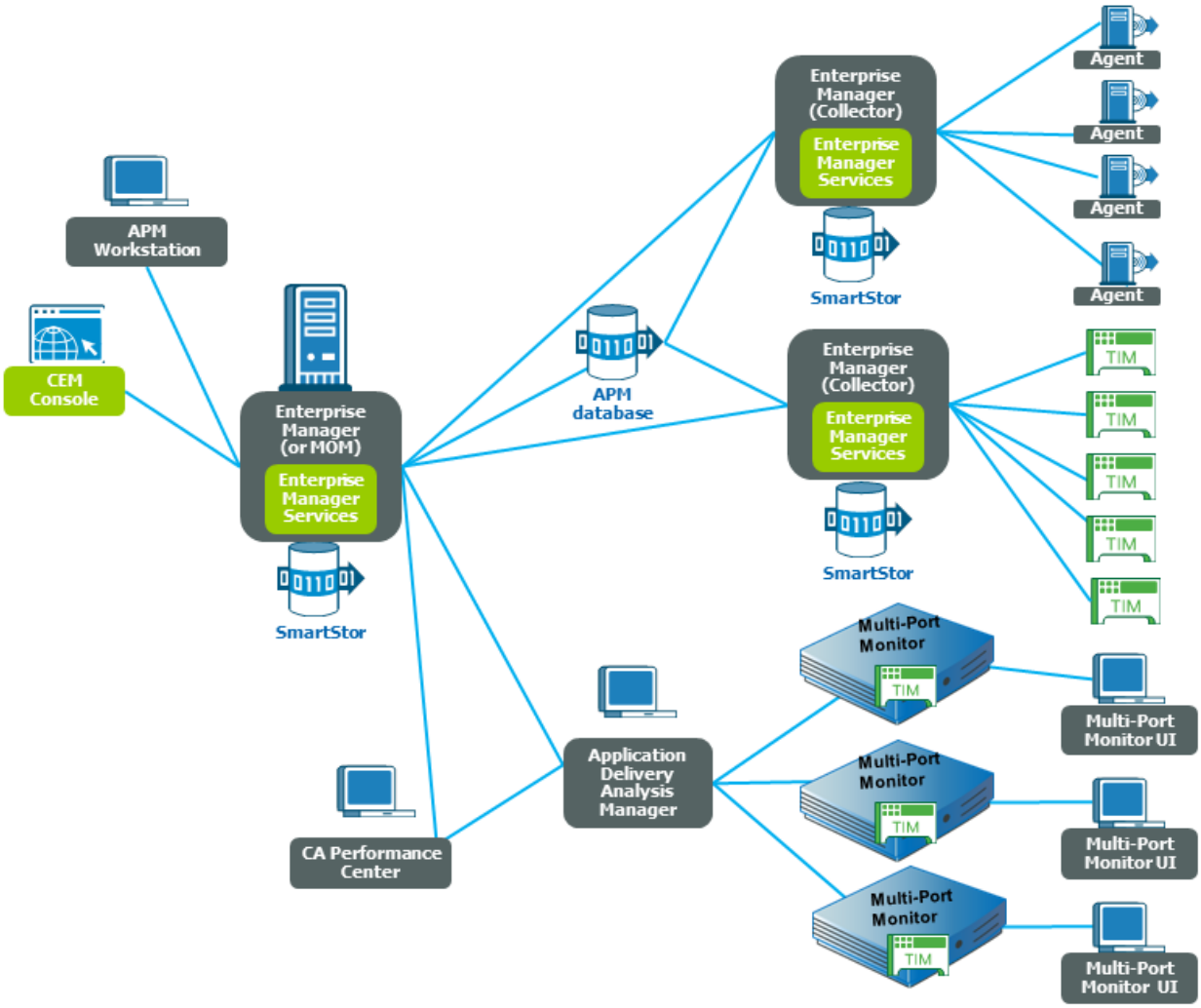
Figure 1: Deployment architecture with a single multi-port monitor.



In more complex environments where multiple Multi-Port Monitors are required, you can scale up to:

- Ten Enterprise Manager Collectors
- Five Multi-Port Monitors
- Five standalone TIMs

More complex environments typically require a clustered CA APM environment with multiple Multi-Port Monitors. In a clustered CA APM environment, multiple Enterprise Managers (called Collectors when clustered) collect all agent metrics. You can subscribe to metrics from all the Enterprise Manager Collectors and the Manager of Managers (MOM) Enterprise Manager. In addition, the MOM manages cluster functions. For example, the MOM handles all Workstation requests for data and gathers those requests from the collectors. In a clustered environment, your deployment architecture may look similar to the following diagram.



Single Sign-On

Single Sign-On is the authentication scheme for CA Performance Center and all supported data sources. After users are authenticated to CA Performance Center, they can navigate among the consoles and registered data sources without signing in a second time.

Note: Single Sign-On is not supported with CA APM Workstation.

CA Performance Center uses a distributed architecture. An instance of the Single Sign-On web site is automatically installed on every server where a supported data source or CA Performance Center is installed. If two data source products are installed on the same server, they use the same instance of the Single Sign-On web site. The distributed architecture lets users log in to individual CA data source products by logging in to the servers where these products are running.

Note: For more information about Single Sign-On, see the *CA Performance Center Administrator and User Guide.*

CA SiteMinder Support

If you have SiteMinder installed on your application servers, then configure TIM to allow for transaction monitoring. If TIM is not configured properly, it ignores all transactions originating from those application servers.

Note: For more information about configuring TIM for transaction monitoring with SiteMinder, see the *CA APM Configuration and Administration Guide*.

More Information

You can refer to the following documentation and resources:

- *CA APM Installation and Upgrade Guide*

  Intended for the deployment team and system administrators. This guide provides installation and upgrade information for the following components:

  - APM database
  - Enterprise Manager/MOM
  - Workstation
  - Stand-alone TIMs

- *CA APM Configuration and Administration Guide*

  Intended for system administrators. This guide provides configuration and administration information (minus defining application transaction content) for the following components:

  - APM database
  - Enterprise Manager/MOM
  - Workstation
  - Stand-alone TIMs

- *CA APM Transaction Definition Guide*

  Intended for system administrators. This guide covers information about establishing and maintaining business applications, business services, and transaction definitions.

- *CA APM Java Agent Implementation Guide*

  Intended for system administrators. This guide covers information about installing and configuring Java agents.

- *CA APM .NET User Guide*

  Intended for system administrators. This guide covers information about installing and configuring .NET agents.

- *CA APM Workstation User Guide*

  Intended for system administrators and system analysts. This guide covers information about using the Workstation to triage your application.

- *CA APM Sizing and Performance Guide*

  Intended for system administrators. This guide provides information about hardware sizing and system performance that is based on your sizing decisions.

- *CA Multi-Port Monitor Installation Guide*

  Intended for system administrators. This guide covers information about installing the Multi-Port Monitor software.

- *CA Multi-Port Monitor Upgrade Guide*

  Intended for system administrators. This guide covers information about upgrading the Multi-Port Monitor software.

- *CA Multi-Port Monitor User Guide*

  Intended for system administrators and analysts. This guide covers information about configuring, administering, and using the Multi-Port Monitor.

- *CA Performance Center Installation Guide*

  Intended for system administrators. This guide covers information about installing the CA Performance Center software.

- *CA Performance Center Administrator and User Guide*

  Intended for system administrators and analysts. This guide covers information about administering and using the CA Performance Center.

Chapter 2: Planning the Deployment

This section contains the following topics:

Deployment Considerations

Before you install or upgrade, carefully plan your deployment. The following list outlines some important steps to consider:

- Evaluate your existing environment and determine how and where you plan to deploy the necessary components.
- Identify the characteristics of the environment you want monitored.
- Understand your SPAN or mirror port options for the converged appliance. The Multi-Port Monitor connects through a SPAN or mirror port to the key switches carrying application traffic to your network.

  Note: For more information about mirror port options in relation to the converged appliance, see the *CA Multi-Port Monitor User Guide*.
- Understand your mirror port options for the standalone TIM. A standalone TIM connects to a mirrored port or a network tap. This configuration ensures that TIM can monitor your network traffic without interfering with your data transmission.

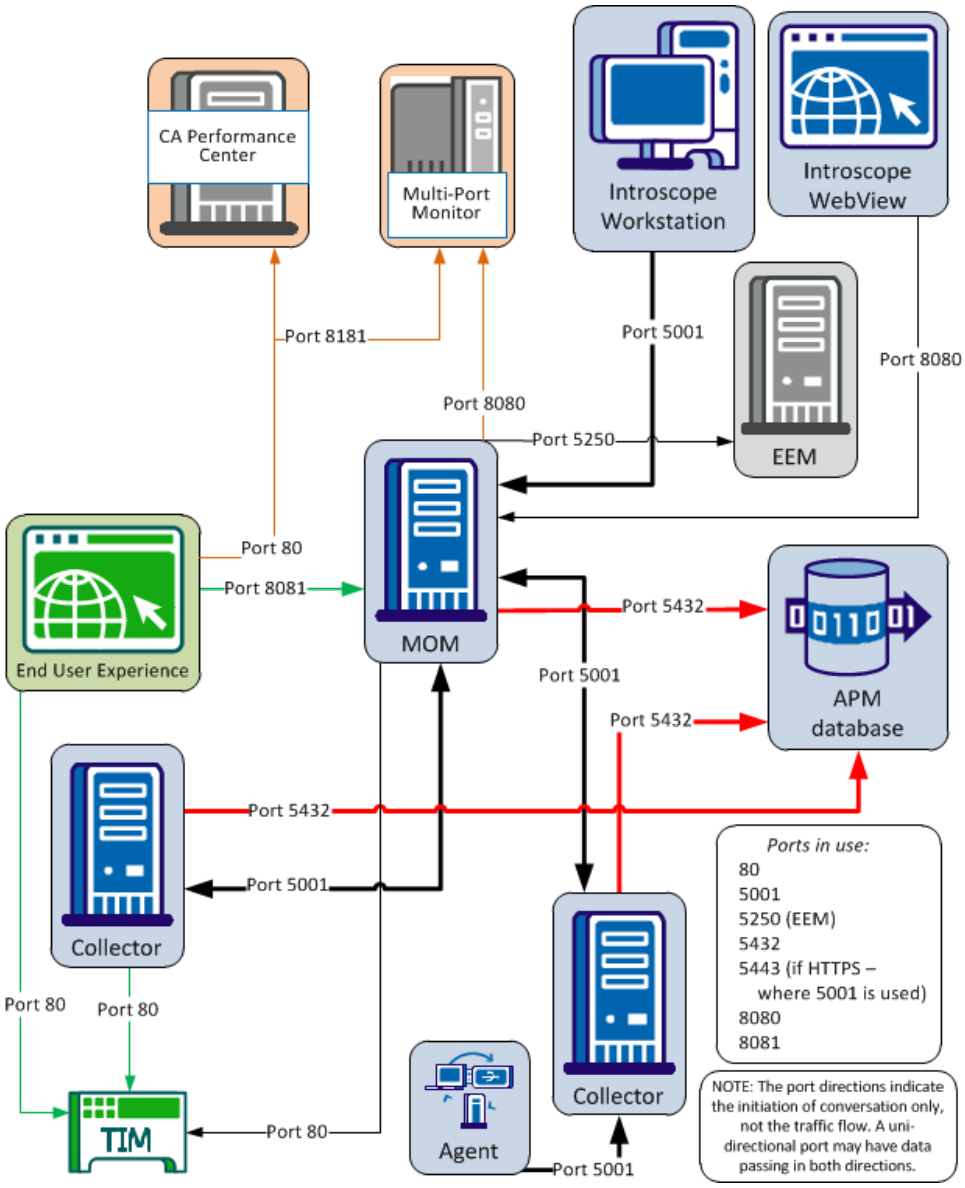
  Note: For more information on mirrored ports and network taps in relation to the standalone TIM, see the *CA APM Configuration and Administration Guide*.
- Gather server IP addresses and application port numbers. The IP addresses and application ports you want monitored in your enterprise network are required to configure the switch SPAN or mirror sessions.

  Note: For more information about ports and protocols for Multi-Port Monitor, see the *CA Multi-Port Monitor User Guide*.
- Review the *CA APM Installation and Upgrade Guide* to understand the requirements for the following CA APM components:
  - APM database
  - Enterprise Manager

  - CA CEM console
  - Workstation
  - Stand-alone TIM
- Review the *CA APM .NET Agent Implementation Guide* for .NET agent installation requirements.
- Review the *CA APM Java Agent Implementation Guide* for Java agent installation requirements.

Port Considerations

CA APM and CA Infrastructure Management components require certain ports through which communication takes place. The following diagram shows these components and ports.



Note: When TIM is installed on Multi-Port Monitor, it communicates with the MOM Enterprise Manager through Multi-Port Monitor on port 80. Port 8080 uses MOM Enterprise Manager to communicate with Multi-Port Monitor.

Component Requirements

The following components are required for a successful deployment:

- CA Multi-Port Monitor 2.2
- CA APM TIM version 9.1 compiled for 64-bit CentOS 5.5
- CA Performance Center version 2.0.00

  Important! Other versions of CA Performance Center are *not* supported for integration with CA APM.
- APM database 9.1 or newer
- Enterprise Manager 9.1 or newer
- CA APM Workstation 9.1 or newer
- *One* of the following:
  - CA APM .NET agent 9.0 or newer
  - CA APM Java agent 9.0 or newer

Note: For detailed hardware and installation requirements specific to each component, see the corresponding installation guides.

Multi-Port Monitor

Multi-Port Monitor is a hardware appliance which includes the following:

- High-performance capture card
- 4-disk RAID array used for the system and database
- 12-disk RAID array used to store packets

Multi-Port Monitor is a high capacity monitor that groups multiple packet collections into one appliance. Multi-Port Monitor includes both hardware and software components. The hardware component is a 16 disk server that captures and processes traffic flowing into and out of a switch. The software component is an administrative web interface lets you perform maintenance tasks, check the status of collection on the device, and build custom views.

Note: For installation and information, see the *Multi-Port Monitor Installation Guide.* To upgrade the Multi-Port Monitor software for the converged appliance, see the *CA Multi-Port Monitor Upgrade Guide*.

Deployment Scenarios

Your deployment path depends on the CA Technologies components currently running. For example, if the Enterprise Manager, APM database, .NET agents, and the Workstation are running, then perform the following tasks:

- Upgrade your existing CA APM components
- Install TIM on the Multi-Port Monitor

If you have existing standalone TIMs, you have the following options:

- Keep the standalone TIMs.
- Upgrade the TIMs, and reconfigure each TIM (including the new TIM on Multi-Port Monitor) to monitor specific network traffic and load balance the traffic among the TIMs.
- Remove your stand-alone TIMs and move the SPAN for them to the new TIM on Multi-Port Monitor.

Deploy Unified End-User Monitoring into a New Environment

Use this scenario if you are new to the CA APM transaction and CA Infrastructure Management solutions. This scenario provides the high-level steps to ensure a successful deployment of Unified End-User Experience Monitoring.

Follow these steps:

1. Carefully plan your deployment (see page 21).
2. Set up the Multi-Port Monitor appliance and install the software using the *CA Multi-Port Monitor Installation Guide* and the *CA Multi-Port Monitor User Guide*.
3. Install TIM on the Multi-Port Monitor (see page 30).
4. Configure TIM monitoring (see page 36) from the Multi-Port Monitor web interface.

   On the converged appliance, TIM supports monitoring from a single logical port. You can map multiple physical ports to a single logical port.
5. Configure hardware filters (see page 33).
6. Install the following CA APM components using the *CA APM Installation and Upgrade Guide* for installation instructions:
   - APM database 9.1 or newer
   - Enterprise Manager 9.1 or newer
   - Workstation 9.1 or newer
   - Java or .NET agents 9.0 or newer

7. Associate TIM with an Enterprise Manager (see page 38).

   This task is performed in the CA CEM console and enables TIM to communicate with an Enterprise Manager. Perform this task for all TIMs—standalone TIMs (if applicable) and TIM running on Multi-Port Monitor.

8. Configure web server filters (see page 40) (optional).
9. Create transaction definitions (see page 41).
10. Create alerts for application triage map elements (see page 41).
11. Install CA Performance Center (see page 44).
12. Install the CA Performance Center Integration Pack (see page 44).
13. Start the APM-CAPC service (see page 46).
14. Import the APM views (see page 46) into the CA Performance Center database.
15. Register CA APM as a data source (see page 47) on the CA Performance Center.
16. Add the APM dashboards (see page 48) to the Application Health menu in CA Performance Center.
17. Enable HTTPS support (see page 49) (optional).
18. Verify the deployment (see page 51) by displaying data in the relevant interfaces and reporting consoles.

Deploy Unified End-User Experience Monitoring into an Existing Environment

If you have an existing CA APM deployment, evaluate your deployment and install or upgrade the relevant components. In addition, install Multi-Port Monitor and its associated infrastructure management components. This scenario outlines the high-level steps to ensure a successful deployment of Unified End-User Experience Monitoring.

Follow these steps:

1. Carefully plan your deployment (see page 21).
2. Set up the Multi-Port Monitor appliance and install the software using the *CA Multi-Port Monitor Installation Guide* and the *CA Multi-Port Monitor User Guide*.
3. Install TIM on the Multi-Port Monitor (see page 30).
4. Configure TIM monitoring (see page 36) from the Multi-Port Monitor web interface.

   On the converged appliance, TIM supports monitoring from a single logical port. You can map multiple physical ports to a single logical port.

5. Configure hardware filters (see page 33).
6. Upgrade the following CA APM components using the *CA APM Installation and Upgrade Guide* for installation instructions:
   - APM database 9.1 or newer
   - Enterprise Manager 9.1 or newer
   - Workstation 9.1 or newer
   - Java or .NET agents 9.0 or newer
7. Associate TIM with an Enterprise Manager (see page 38).

   This task is performed in the CA CEM console and enables TIM to communicate with an Enterprise Manager. Perform this task for all TIMs -- standalone TIMs (if applicable) and TIM running on Multi-Port Monitor.
8. Configure web server filters (see page 40) (optional).
9. Create alerts for application triage map elements (see page 41).
10. Uninstall any previous version of CA Performance Center Integration Pack using the instructions in the corresponding installation guide.
11. Install CA Performance Center (see page 44).
12. Install the CA Performance Center Integration Pack (see page 44).
13. Start the APM-CAPC service (see page 46).
14. Import the APM views (see page 46) into the CA Performance Center database.
15. Register CA APM as a data source (see page 47) on the CA Performance Center.
16. Add the APM dashboards (see page 48) to the Application Health menu in CA Performance Center.
17. Enable HTTPS support (see page 49) (optional).
18. Verify the deployment (see page 51) by displaying data in the relevant interfaces and reporting consoles.

Chapter 3: Deploying the Components

This section contains the following topics:

Set Up and Install the Multi-Port Monitor

To install and configure the Multi-Port Monitor appliance and install the software, see the *CA Multi-Port Monitor Installation Guide*. Multi-Port Monitor software for the converged appliance. To upgrade the Multi-Port Monitor software, see the *CA Multi-Port Monitor Upgrade Guide*.

Note: After you configure the hardware and install the Multi-Port Monitor software, install the TIM software bundle. Installing TIM on the Multi-Port Monitor allows it to function as a converged appliance.

TIM on the Multi-Port Monitor

TIM lets system administrators configure Multi-Port Monitor appliances to function as converged appliances. The converged appliance lets you collect TCP and HTTP data and passes these packets to TIM. The Multi-Port Monitor converged appliance provides visibility into application and infrastructure performance metrics related to application usage by end-users.

The following table identifies the differences between TIM installed on the Multi-Port Monitor and standalone TIM.

TIM on the Multi-Port Monitor	Standalone TIM
Runs on 64-bit CentOS Linux 5.5	Runs on 64-bit Red Hat Linux 5.5
Runs in multi-process mode to increase throughput	Runs in single-process mode

TIM on the Multi-Port Monitor	Standalone TIM
Reads packets from files written by the Multi-Port Monitor capture layer	Reads packets directly from the NIC
Time is derived from the packet timestamps. The Napatech card (using the Napatech clock) time-stamps packets as they enter the Multi-Port Monitor.	Time is derived from the system time (wall clock)
Napatech or network card not required because the Multi-Port Monitor has its own Napatech card installed.	Requires purchase of a Napatech or network card.
Uses the following default log-on credentials: User name: nqadmin Password: nq	Uses the following default log-on credentials: User name: cemadmin Password: quality

Install TIM on the Multi-Port Monitor

Install these two files in the following order to install TIM on the Multi-Port Monitor. These files are CentOS-specific images required for the Multi-Port Monitor.

1. Third-party image: APMCOSTRDPRTxxxx.img
2. TIM image: APM_COSTIMCMxxxx.img

The TIM software DVD bundle or the CA APM software download area on CA Support contains these software images. Mount the DVD onto your network to access them from the Multi-Port Monitor appliance.

Before you start the installation, verify that Multi-Port Monitor is configured and connected to the network.

Follow these steps:

1. Log on to the Multi-Port Monitor using your administrator credentials or the following if you have not changed the default:

   Username = nqadmin

   Password = nq
2. Click System Setup tab.
3. Click Install Software tab.

   The Install Software page opens.

4. Install the third-party software.
   a. Click Browse and navigate to the TIM install files.
   b. Select the APMCOSTRDPRTxxxx.img file.
   c. Click Upload and Install.
   d. Read and accept the License Agreement.

      Accept the EULA to continue.
   e. The software installation log appears. If you see errors, contact CA Support.

      The third-party software is installed.
5. Install the TIM software.
   a. Click Install Software tab.
   b. Click Browse and navigate to the TIM install files.
   c. Select the APM_COSTIMCMxxxx.img file.
   d. Click Upload and Install.
   e. Read and accept the License Agreement.

      Accept the EULA to continue.
   f. The software installation log appears. If you see errors, contact CA Support.

      The TIM software is installed.
6. (Optional) Click the System Setup tab to see a list of packages installed or the Administration tab to enable TIM Monitoring on a Multi-Port Monitor logical port.
7. Restart the Multi-Port Monitor.

TIM in Multi-Process Mode

When TIM is installed on the Multi-Port Monitor, it can utilize the multiple CPUs and load balance the traffic among multiple processes. Running in multi-process mode increases TIM throughput significantly. Exact throughput numbers vary based on many factors, such as the traffic being monitored, how you define transactions, and more.

In multi-process mode, TIM splits network traffic among multiple processes called worker processes. For TIM in multi-process mode to work effectively, do the following:

- Distribute monitored traffic as evenly as possible between worker processes
- Verify the same worker process monitors all packets belonging to same business transaction instance

In different network configurations, these guidelines can be achieved by different means. CA Technologies provides several flexible ways to distribute traffic between workers. Options are:

Client IP address option

Network traffic is assigned to worker processes based on the client IP address. This is the default and CA Technologies recommended option. Consider the other options if your network configuration does not make this option viable. For example, if all traffic appears to be coming from the same client IP address, such as when TIM is positioned behind a proxy server, then consider the other configuration options. The default configuration for this example is shared=client. Load balancing on TIM is not possible with this network configuration, so consider using the server IP address option.

Sever IP address option

Network traffic is assigned to worker processes based on the server IP address, for example shared=server. This option requires that a single server handles all transactions in a business transaction.

Mixed option

Traffic can be assigned to worker processes based on a combination of client and server IP addresses. If there is a discrepancy between the server rule and client rule, then the server rule takes precedence.

Use the Load Balancer Configuration file to define how you want TIM to load balance your clients or servers. It is a plain text file.

Note: Standalone TIMs run in single-process mode.

Examples: Configure TIM to Run in Multi-Process Mode

The following examples show configuration options for setting up TIM in multi-process mode. Make these configuration changes on the balancer.cnf file, located in /etc/wily/cem/tim/config/. Restart TIM to activate these configuration changes.

Example 1

For a client with HTTP transactions belonging to the 138.42.123.*/24 subnet, use the following configuration to assign worker process 0 to this subnet: client=138.42.123.*/24 worker=0.

Example 2

If you have a server in the 138.42 subnet, use the following configuration to assign worker process 0 to this subnet: server=138.42.0.0/16 worker=0.

Edit Load Balancer Configuration File

Edit the Load Balancer Configuration file to define how you want TIM to load balance your clients or servers.

Follow these steps:

1. Log in to the converged appliance (Multi-Port Monitor running TIM).
2. Open the balancer.cnf file using a text editor.

   The file is located in /etc/wily/cem/tim/config/balancer.cnf.

   Do **not** use a Word processor or other programs that add formatting information.
3. Edit and save the file.
4. Restart TIM.

Configure Hardware Filters

Hardware filters can further refine the data that is processed from your switches and thus optimize Multi-Port Monitor performance.

Specific to the Unified End User Experience Monitoring solution, web traffic monitored by TIM must have full packets. You can define full packet capture by editing a default filter called "HTTP-full packets" from the Multi-Port Monitor web UI. You receive a warning message on the Logical Ports page if TIM monitoring is enabled on a logical port in which all filters are slicing packets.

You can create, enable, disable, and modify predefined filters or the filters you create.

Follow these steps:

1. Click Administration, Logical Ports in the web interface.

   The Logical Ports page opens.
2. Click the Filters link in the Edit Filters column for the logical port you want to filter.

   The Logical Ports: Hardware Filters page opens.
3. Perform one of the following tasks:
   - Click New to create a filter. The Logical Ports: New Hardware Filter page opens.
   - Click Edit to modify or enable a filter. The Logical Ports: Edit Hardware Filter page opens.

4. Complete the following fields:

   - **Filter Enabled**. Applies the filter on the logical port whose name is indicated. If selected, the filter is applied after you restart the nqcapd process.
   - **Filter Name**. The name of the filter you are creating or editing. The filter name is shown on the Hardware Filters page for the logical port to which it is applied.
   - **Filter Priority**. Priority determines which filters take precedence when filter criteria overlap. That precedence is undefined when two or more overlapping filters have the same priority. Values range from 0 (highest priority) to 62 (lowest priority). The default priority is 10.

     Filter priority settings can be used with packet slicing. For example, you want to keep more bytes of each HTTP packet. You specify a filter for TCP and Port 80 with slicing set to TCP headers + 50 bytes and Priority set to 1. You then apply a separate filter for TCP with slicing set to TCP headers + 1 byte and Priority set to 10. In this scenario, more payload bytes are kept for HTTP traffic than for other TCP traffic.

     Packet Slicing Mode. Options for capturing only selected parts of each packet. The hardware filters let you capture packets for protocols other than TCP/IP. However, Multi-Port Monitor collects performance metrics only for TCP traffic. Volume metrics are collected for all traffic types.

     - Capture full packet: All information is captured from each packet that passes the filter.
     - Capture fixed size: Some bytes are captured from every packet. In the Packet Slicing Size field, supply the number of bytes to capture.
     - Capture headers plus size: All Layer 2, Layer 3, and Layer 4 headers are captured, plus the fixed number of payload bytes from the Packet Slicing Size field.
       -- Layer 2 headers include Ether II, LLC, SNAP, and Raw headers, and VLAN, ISL, and MPLS tags.
       -- Layer 3 headers include IPv4 (including IPv4 options), IPv6, and IPX headers.
       -- Layer 4 headers include TCP, UDP, and ICMP headers.
   - **Include only Protocols**. Limits the protocols to capture and process. Only the selected protocols are included in monitoring. If no check boxes are selected, all protocols are included.
     - TCP: Transport Control Protocol, which is the main protocol that CA Application Delivery Analysis monitors.
     - UDP: User Datagram Protocol, which is used for transport of the data that real-time or streaming applications send.
     - ICMP: Internet Control Message Protocol, which is used for error messaging among servers and for CA Application Delivery Analysis traceroute investigations.

- **VLANs**. The identifiers of the virtual local area networks (VLANs) to monitor or exclude from monitoring. List the identifiers of VLANs whose traffic passes through the indicated logical port. Separate multiple VLANs with commas and no spaces. Select Exclude to discard traffic from the VLANs you listed.
- **Subnets**. The subnets to monitor or exclude from monitoring. Supply a valid IP address and subnet mask. Specify the number of bits to use for the mask. Use the following format: 10.9.8.0/24. Select Exclude to discard traffic from the subnets you listed.
- **IP Addresses**. The IP addresses of individual hosts to monitor or exclude from monitoring. Separate multiple IP addresses with commas and no spaces. Use dotted notation for the format, such as 10.9.8.7 or 10.9.8.7,10.9.8.5,10.9.7.7. Select Exclude to discard traffic from the IP addresses you listed.

  Ports. The TCP ports or port ranges to monitor or exclude from monitoring. Separate multiple port numbers with commas and no spaces. For a range of ports, use the following format: 2483-2484. Select Exclude to discard traffic from the ports you listed.

5. (*Optional*) Click Show Details to view your selections as a regular expression.
6. (*Optional*) Click Advanced to use regular expressions to create more precise filters. For more information, see Use Regular Expressions for Precise Filtering.
7. Click Save.

   The new filter appears on the Logical Ports: Hardware Filters page.
8. Restart the nqcapd process if you enabled a filter.

Turn On/Off Multi-Process Mode

You can turn the multi-process mode on/off from the TIM configuration window. The mode is turned on by default.

Follow these steps:

1. From the Multi-Port Monitor UI, select System Setup.
2. Select Tim x.x.x.x build xx.

   The Tim Setup page opens.
3. Select Configure TIM Settings

   The Tim Settings page opens.
4. Select Parallel/UseWorkers.
5. Change the New Value field accordingly.

   1 means multi-process mode is on.

   0 means multi-process mode is off.
6. Restart TIM.

   You must restart TIM to make this change effective.

Configure TIM Monitoring on Logical Port

TIM monitors mirrored ports from one logical port, despite the availability of multiple logical ports on the Multi-Port Monitor appliance. To map multiple physical ports to one logical port, mirror the web traffic from the WAN to the logical port. This traffic is processed for TIM and CA Application Delivery Analysis. Use the other logical ports for other port mirroring, ideally from the access-layer switches closest to the servers. The non-TIM logical ports are processed for CA Application Delivery Analysis only.

Follow these steps:

1. Open a browser window and log in to the Multi-Port Monitor web interface.

   The Multi-Port Monitor web interface opens.

2. Click the Administration tab.

   The Logical Ports page opens. The default settings for the available ports are shown.

   1. Click the Filters link in the Edit Filters column to apply hardware filters (see page 33) to the port.
   2. Provide the following information:

      Name

      Specifies the name of the logical port you want TIM to monitor.

      The name helps to identify the source of the traffic you are monitoring. For example, use the name or location of the switch you are monitoring.

      Enabled

      Enables the port for monitoring.

      Confirm that the check box labeled Enabled is selected.

      Save Packets to Disk

      (Optional) Saves captured data packets on the Multi-Port Monitor hard disk drive. With this option, the data may be available for export to PCAP on the Analysis page. By default, the Multi-Port Monitor keeps the packet for six hours.

      TIM Monitor

      Associates with the logical port you are configuring.

      Select the check box associated with the logical port you are configuring.

      Physical Ports

      Assigns one or more of the available Physical Ports to the logical port.

      The available ports depend on the capture card configuration you purchased from CA Technologies.

      Logical port numbering begins at 0. The capture layer performs the mapping of physical ports to logical ports. The mapping process is transparent to TIM.

3. Click Save.

4. Restart the nqcapd process.

   Perform this task on the Multi-Port Monitor Processes page.

5. (Optional) Check the status of the logical ports by viewing the Capture Card Logical Port Status table on the System Status page.

   The Status column shows an Error status if there is a problem with starting the logical port, such as a syntax error in a hardware filter associated with that port.

Associate TIM with an Enterprise Manager

This task is relevant to both the TIM on the Multi-Port Monitor and standalone TIMs (if applicable).

Enable the TIMs so that the TIMs can monitor transactions. The Enterprise Manager does not receive data from disabled TIM monitors. If you have clustered Enterprise Managers, then enable the TIMs from the MOM Enterprise Manager.

These are some examples of when you need to enable TIMs:

- When setting up a TIM and associating it with an Enterprise Manager.
- After upgrading the TIMs and/or Enterprise Manager.
- After a configuration is imported.

Follow these steps:

1. Open a web browser and enter the address of the server that hosts the Enterprise Manager. If using a clustered environment, specify the address of the MOM:
   `http://<IP_Address>:8081/wily`

   where *<IP_Address>* is the IP address or DNS name for the MOM or a standalone Enterprise Manager. For example:
   `http://192.168.1.54:8081/wily`
   `http://cem.company.com:8081/wily`

   To use a DNS name, your DNS administrator must have configured it.

   Note: The default port is 8081. It is defined in the *IntroscopeEnterpriseManager.properties* file as *introscope.enterprisemanager.webserver.port=8081* and can be changed.

2. Enter the user name and password.

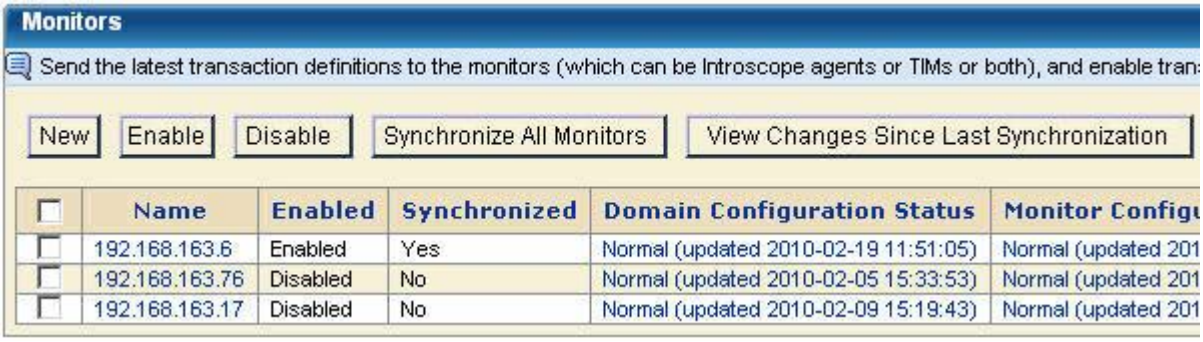
   The CEM console appears.

3. Select Setup, Monitors.

4. If the TIM does not appear in the list:
   a. Click New.
   b. Enter the name and IP address of the TIM.
   c. Select the Multi-Port Monitor Enabled check box if TIM is listening on Multi-Port Monitor ports.

      This task is only applicable if you are deploying the Multi-Port Monitor.
   d. Click Save.
5. Select the check box next to each required TIM and click Enable.

   Communication between the Enterprise Manager and the TIMs is then enabled. Additional tabs appear in the CA CEM console as follows:



Install CA APM

Install and configure each of the following CA APM components to ensure a successful deployment:

- APM database
- Enterprise Manager
- Workstation
- *One* of the following components
  - CA APM Java Agent
  - CA APM .NET Agent

More information:

Component Requirements (see page 24)

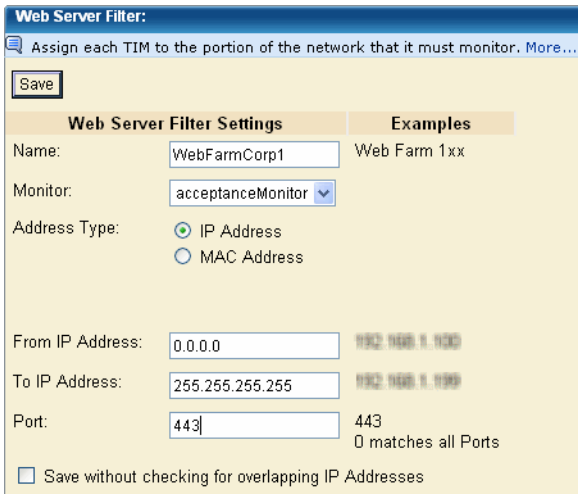
Configure Web Server Filters

This task is optional. Perform this task if you still see too much network traffic after you have configured hardware filters. In this case, you need to further restrict the traffic monitored by TIM to specific servers by configuring web server filters. If TIM gets overloaded, recording might not work.

Multi-Port Monitor uses the web server filter configured for TIM running on the appliance to define what data it forwards to TIM.

Follow these steps:

1. Open the CEM console.
2. Select Setup > Web Server Filters.
3. Click New.
4. Type a Name that describes the network portion for TIM monitoring. For example, *WebFarmCorp1*.



5. In the Monitor list, select the TIM to assign to monitor this portion of the network.

   Each TIM monitors an IP address range by default. If you want to monitor using a specific MAC address instead, go to step 6.

   a. Fill in the From IP Address field.

      Type the IP address of the Web server at the low end of the range. If there is only one server to monitor, type the specific IP address.

   b. Fill in the To IP Address field.

      Type the IP address of the Web server at the high end of the range. If there is only one server to monitor, type the specific IP address.

c. Fill in the Port field.

- If the TIM is to monitor transactions only on a specific port, type the port number.
- If the TIM is to monitor all transactions on all ports, type 0 (the default).

d. In most cases, TIMs should monitor specific servers in the network rather than overlapping servers. However, in special circumstances, you can allow overlapping IP addresses.

If you want to configure more than one monitor for an IP address or range, select Save without checking for overlapping IP Addresses.

6. If you want to monitor a specific MAC address instead of by IP address range:

a. Click the Address Type of MAC Address.

b. Type the specific MAC Address of the device you want to monitor. For example: 12:eb:a0:32:51:4c.

7. Click Save to configure the TIM monitor as specified.

Create Transaction Definitions

Transaction identification is the process of defining unique transactions that can be distinguished from other transactions. This process provides a way of refining unique transaction signatures for use by CA APM. For example, a user logs on to your site and submits a form to the HR department. Correctly specified transaction definitions enable the system to identify the user login transaction and the HR form submission transaction as two distinct transactions.

CA APM provides multiple options for you to create transactions:

- Manually create your transactions
- Let CA APM automatically discover transactions
- Let CA APM record transaction signatures on your network and use them as templates to generate transaction definitions

Note: For more information about creating business transactions, see the *CA APM Transaction Definition Guide.*

Create Alerts from Application Triage Map Elements

From the Workstation, create alerts on the application map elements for application, business service, and business transaction health status indicators. These alerts are baselines for the health statuses in CA Performance Center. You create alerts to display application, business service, and business transaction health status indicators in CA Performance Center.

Follow these steps:

1. Right-click a frontend, backend call, or other alertable element in the map or tree.
2. Select *Edit Alert for <Object_Name>...*
3. In the left pane, identify a metric you want to contribute to alert status.
4. From the Problem drop-down, select the Problem you want to trigger the alert. Available values are:
   - Value Too High -- The alert will trigger when the metric value exceeds the threshold.
   - Specific Bad Value(s) -- The alert will trigger when the metric value is equal to the threshold, and subsequently the threshold will be referred to as "Bad Value" rather than "Threshold Value."
   - Value Too Low -- The alert will trigger when the metric value drops below the threshold.
   - Unexpected Values -- The alert will trigger when the metric value is not equal to the threshold value, which subsequently will be referred to as "Expected Value" rather than "Threshold Value."
5. In the Summary Tab of the Threshold Settings region:
   a. Set the Threshold Values for Danger and Caution alerts.
   b. Set the Sensitivity Levels for Danger and Caution alerts. Available values are:
      - High -- For Danger threshold, 1 value in 1 sample. For Caution, 1 value in 1 sample.
      - Medium -- For Danger, 2 values in 2 samples. For Caution, 2 values in 2 samples.
      - Low -- For Danger, 4 values in 4 samples. For Caution, 4 values in 4 samples.
      - Custom... -- This allows you to set your own sensitivity levels using the Select Custom Sensitivity Settings dialog.

      Note: See the note on custom threshold settings below.

6. Optional: setting different or less sensitive thresholds on Locations.

   The Location settings by default are the same as Summary but can be modified to their own unique values. This would allow, for example, different settings on an individual location/agent level versus the total aggregated metric value. Suppose there are 100 agents and one is performing badly. You might miss this anomaly in a Summary level alert where the aggregated value across all agents is still within normal range. But if you set a more restrictive range on a per agent basis, to alert you that a location has stopped performing, you are more likely to spot the poorly performing location.

   To set varying values on Locations:

   a. Select the Locations tab.

   b. Set different threshold values for the locations which report the metric.

   c. Click *Apply.*

7. Optional: The Properties tab allows you to:

   - Enter a description for the alert.
   - Disable the alert by selecting Disabled (all). This disables all individual contributing alerts AND the object alert as a whole.
   - Configure the Interval.
   - Select *Location alerts contribute to overall status.*

   Note: By default, the map object will display the alert state only if its summary metric is alerting; to see if any individual location is alerting, you must view the Locations table. If selected, the Location alerts contribute to overall status option means that a frontend's alert will include the alerts for each of its locations. Thus, if any single location of the frontend is alerting, the map will show an alert state.

8. Optional: Use the Actions tab on the Creating and Editing Alerts dialog to add an action to the alert or to display Location alerts in the Alert Details panel.

Note on Custom Sensitivity Threshhold Settings

When you select Custom in the Sensitivity Threshold dropdown, you can define your own settings. If you happen to use settings that match those of one of the pre-configured levels, then the dropdown will show the pre-configured level. For example, if you select custom and then enter the same settings as "Medium," then the dropdown will show Medium.

Workstation doesn't store the Level designation in the alert definition, only the specific sensitivity configuration settings. The UI assigns the level (Low, Med, High, Custom) on the fly by comparing the stored config settings against pre-defined definition of these levels. Helper text is displayed in blue type as you set sensitivity levels, helping you understand your settings.

Install CA Performance Center

CA Performance Center version 2.0.00 is required for the integration with CA APM. To install CA Performance Center, see the *CA Performance Center Installation Guide*.

Important! Uninstall any previous version of CA Performance Center Integration Pack using the instructions in the corresponding installation guide.

Install CA Performance Center Integration Pack

The CA Performance Center Integration Pack installer program enables the following key feature of the Unified End User Experience Monitoring solution:

- Viewing application data on the CA Performance Center

Before you begin, verify that you have installed and configured:

- CA APM and the Enterprise Manager
- Alerts on the Workstation application triage map elements
- Agents to monitor business transactions, business services, and business components

CA Performance Center Integration Pack

Application data flows from the Enterprise Manager to the CA Performance Center. This integration pack provides CA APM data in a format that CA Performance Center can understand and display.

You need the following information to complete the installation:

- Enterprise Manager host name
- Enterprise Manager web server port number
- CA APM Workstation user name
- CA APM Workstation password
- Enterprise Manager services user name and password
- Web server port that CA Performance Center Integration Pack uses

The CA Performance Center Integration Pack installable component installs the APM-CAPC service.

Run the Installer Program

The CA Performance Center Integration Pack installer program enables communication between CA Performance Center and CA APM. This installer program contains two installable components, CA Performance Center Integration Pack and CA Application Delivery Analysis Extension for APM.

Install on the Enterprise Manager or MOM (if you have a clustered CA APM environment).

Follow these steps:

1. Download the CA Performance Center Integration Pack installer for Application Delivery Analysis program from the CA APM software download area on CA Support.
2. Navigate to your local version of the CA Performance Center Integration Pack installer program and double-click it.

   The installer opens.
3. Click Next on the Welcome screen.
4. Read and accept the End User License Agreement.

   Accept the agreement to continue.
5. Specify where you want the integration pack files installed and click Next.
6. Select one or both of the following installable components:
   - CA Performance Center Integration Pack
   - CA Application Delivery Analysis Extension for APM

   Important! If you select CA Application Delivery Analysis Extension for APM, then you are prompted for information about the ADA integration. For more information about NetQoS Performance Center and ADA, see the corresponding product integration guide.
7. Click Next.
8. Specify the Enterprise Manager hostname and webserver port and click Next.
9. Specify the CA Introscope and TESS account of the Enterprise Manager and click Next.
10. Specify whether to configure the CA Performance Center Integration Pack as a Windows service and click Next.
11. Specify the web server port for use by the CA Performance Center Integration Pack and click Next.

12. Review your settings and click Install.

After you install the CA Performance Center Integration Pack installable component, the CAPCIntegrationPack folder appears in the directory specified in step 5. The folder contains the webapps folder, which provides the extracted Jetty Web Server and apm-capc-integration folders.

Start the APM-CAPC Service

After you install the CA Performance Center Integration Pack, start the APM-CAPC service.

Windows OS

Start the APM-CAPC service in Windows Services.

This service does not start automatically. You start it manually after the installation.

Linux/UNIX OS

Start the CA Performance Center Integration Pack using the following command:
`<INSTALL_HOME>\CAPCIntegrationPack\bin$./jetty.sh start`

Import the APM Views into CA Performance Center

Copy the integration XML files and import the APM view definitions into the CAPC database.

Follow these steps:

1. Navigate to the following location:
   `<CAPC Integration Pack Home>\CAPCIntegrationPack\CAPC_2_0`
2. Copy the apm directory from the CAPC_2_0 folder to the plugins folder in the following location:
   `<CAPC-HOME>/PerformanceCenter/SQL/plugins`
3. From a command prompt, execute the following command to import the views into the CAPC database:
   `<CAPC-HOME>/PerformanceCenter/Tools/bin/npcshell.sh dbmigrate –package com.ca.im.plugin.apm –path <CAPC-HOME>/PerformanceCenter/SQL/plugins/apm`

Register APM as a Data Source

CA Performance Center can only receive information from a registered data source.

Follow these steps:

1. Log in to CA Performance Center as a user with administrative privileges.
2. Select Admin, Settings, and click Data Sources.

   The Data Source List page appears.
3. Click Add.

   The Add Data Source page appears.
4. Select Application Performance Management from the Source Type list.

   Note: The Source Type list shows all CA Technologies products that can be registered as CA Performance Center data sources, including products not installed in your environment and some third-party integrations. Supported data sources from other companies are listed only after you complete the required configuration. The Application Performance Management data source supports definition of a single enabled data source. If you want to add another data source, delete the existing data source.
5. Enter the Host Name of the data source.

   The host name is the IP address or DNS host name of the server where the database for this data source is installed. For the CA APM data source, enter the IP address of the host where the CA Performance Center Integration Pack installer program is installed.
6. Select the protocol to use to contact the data source. The default protocol for a CA APM data source is HTTP.

   Select https if your network is using SSL for communications. Verify that you have configured the system correctly before you select the https option.

   Note: If you plan to use SSL for communications between CA Performance Center and the data source products, see the CA Single Sign-on Guide. Specific to the CA APM data source, if you select the https option here, also enable SSL communication between the Enterprise Manager and the integration web services.
7. Supply the port to use when contacting the data source. The port depends on the protocol you selected in the previous step. The default port is 8082 for the Application Performance Manager data source.

   Note: Consult the Single-Sign-On Guide for more information if you plan to use SSL for communications between CA Performance Center and the data source products.
8. Enter a Display Name for the data source. By default, the data source type and the host name are combined to create the name of the data source.
   Example: *<datasourcename>*@*<hostname>*

Note: Web Console address is not applicable to CA APM.

9. Click Save if you have finished registering data sources.

   CA Performance Center lists the data sources registered in the Data Source List.

Add the APM Menu Items to Application Health

In CA Performance Center, add the following CA APM dashboard menu items to the Application Health menu:

- APM - Applications Status
- APM - Business Services Status

Menu items can be added for the default tenant or for any existing tenant. After the menus are set for existing tenants, new tenants can automatically access the menus without the need for these steps.

Follow these steps:

1. Log in as an administrator with the Default Tenant or another Tenant administrator account.
2. Select Admin, User Settings, and click Menus.

   The Manage Menus page displays the current list of menus.
3. Select Application Health and click Edit.
4. Select the APM – Application Summary and/or the APM – Business Services Summary dashboards in the Available list. To select multiple dashboards, use Shift + Click.
5. Click the right arrow.
6. The dashboard moves to the Selected list.
7. Click Save.

   The menu items are set.

Enable HTTPS Support (Optional)

You can enable HTTPS protocol for added security using the Secure Sockets Layer (SSL), which provides communication between CA APM and CA Performance Center as follows:

- Obtain a server certificate. Some administrators can also choose to use client certificates for additional security. Configuring a website in IIS to use SSL, server certificates, and client certificates is outside the scope of this document. However, the following Microsoft article gives an in-depth discussion of the use of these IIS website security features.

  SSL and Certificates (IIS 6.0):
  http://www.microsoft.com/technet/prodtechnol/WindowsServer2003/Library/IIS/559bb9d5-0515-4397-83e0-c403c5ed86fe.mspx?mfr=true

- Configure the CA APM data source with HTTPS support to enable HTTPS communication between the CA Performance Center and CA Performance Center Integration Pack.
- Edit the *apm-capc-integration.properities* file to enable HTTPS communication between the Enterprise Manager and CAPC Integration Pack installable component.

Edit apm-capc-integration.properties File

Editing the apm-capc-integration.properties file enables HTTPS communication between the Enterprise Manager and the CA Performance Center Integration Pack installable component.

Follow these steps:

1. Open the apm-capc-integration.properties file in a text editor from the following location:
   `<INSTALLATION_HOME>\CAPCIntegrationPack\resources`
2. Locate the property: com.apm.npc.em.transport.protocol, and specify the value <*https*>.
3. Locate the property: javax.net.ssl.keyStore, and specify the value <*KEYSTORE LOCATION FOR SSL CONNECTION*>.
4. Locate the property: javax.net.ssl.keyStorePassword, and specify the value <*KEYSTORE PASSWORD FOR SSL CONNECTION*>.
5. Locate the property: javax.net.ssl.trustStore, and specify the value <*TRUSTSTORE LOCATION*>.
6. Locate the property: javax.net.ssl.trustStorePassword, and specify the value <*TRUSTSTORE PASSWORD*>.

   The properties are set.

Chapter 4: Verify the Deployment

This section contains the following topics:

Relevant Interfaces

When you have installed and configured all components, you can view data within the following interfaces:

- CA CEM
- CA APM Workstation
- CA Performance Center
- Multi-Port Monitor user interface

Note: For detailed information specific to each component, see the corresponding product guides.

Data on CEM Console

Application data on the CEM console displays after TIM has been monitoring your network for approximately two hours. Additionally, network data displays on the Defect Details page.

If you do not see application data, verify the following items:

- Communication has been established between TIM and Enterprise Manager.
- Transactions have been defined.
- TIM monitoring has been configured on a Multi-Port Monitor logical port.
- Hardware filter has been configured for that logical port to capture full packets.
- nqcapd process has been restarted.

If you do not see network data on the Defect Details page, verify the following items:

- The Multi-Port Monitor Enabled check-box on the CEM console UI (Monitors, Multi-Port Monitor machine) is enabled to initiate the web service call to the Multi-Port Monitor for the TCP data.
- The defect was generated more than 5 minutes ago. There can be a delay of up to 5 minutes before the network health data is available in the Multi-Port Monitor database. If the defect was generated less than 5 minutes ago, wait a few minutes and then refresh the browser page.

Data on Workstation

Data from the Enterprise Manager displays in the Workstation. To verify the configuration, access the Workstation and view the data from the following locations:

- Overview dashboard accessible from the Console
- Application triage map accessible from the Investigator
- Metric browser accessible from the Investigator

Note: For more information about these features, see the *CA APM Workstation User Guide*.

Data on Multi-Port Monitor

You can use the Multi-Port Monitor user interface to verify that it is capturing data from the expected ports. From the Application default view, you can view data from the Analysis menu. Similar data is available from the Server IP, Client IP, Network, IP Address, and Protocol default views.

Check your port configuration if the data is not available. For more information on port mirroring, see the *CA Multi-Port Monitor Installation Guide*.

Data on CA Performance Center

To verify data in CA Performance Center, view the following dashboards from the Application Health menu accessible from the Dashboard tab:

- APM - Applications Summary (see page 58)
- APM - Business Services Summary (see page 59)

Each dashboard displays a view of data that CA Performance Center receives, interprets, and formats from a registered data source. Each view represents a discrete set of collected data. For example, from the Business Service Status view, you can drill down to more detailed metrics for business transactions, incidents and defects.

Note: For more information about using dashboards, see the *CA Performance Center Online Help*.

Chapter 5: Viewing Application Data in CA Performance Center

This section contains the following topics:

How CA Performance Center Displays Application Data

CA Performance Center displays views of data that it receives, interprets, and formats from a registered data source on report-building dashboard pages. Each dashboard is a collection of views that present data in a graph or chart format. Reports describe the output from each dashboard page. Users can print reports, send them by email, or export them in PDF format. They can also generate a URL for a view and share it with coworkers who do not have access to dashboards.

After the CA Performance Center Integration Pack installation (see page 44) is complete, users can view their application and performance data in CA Performance Center from the following dashboards:

- APM - Applications Summary (see page 58)
- APM - Business Services Summary (see page 59)

They appear on the Application Health menu accessible from the Dashboards tab.

Note: For more information about using dashboards and reports, see the *CA Performance Center Online Help*.

CA APM monitors application health by measuring the performance of individual methods from various application components. Probes that are inserted into application component byte code report data to agents, which in turn report data to the Enterprise Manager. Other subsystems, like JMX and PMI, also report data from agents. Enterprise Manager compiles this data into metrics. CA APM creates associations between applications, business services and business transactions.

Application health and performance status data is sectioned into the following categories:

Applications

Indicates the health status of the applications CA APM monitors. Selecting an application shows the business services being monitored.

Business Services

Indicates the health status of the business services for the selected application. Selecting a business service shows the business transactions CA APM monitors.

Business Transactions

Indicates the health status of the business transactions for the selected business service. Selecting a business transaction displays the customer experience metrics (shown as RTTM) and Business Transaction Component (BTC) Metrics and incidents.

Incidents

Represents the group of defects that are correlated based on transaction type and defect type. Selecting an incident shows the last N (where N = 10 max) defects.

Defects

Displays information specific to each defect. Selecting the web server IP address or client IP address associated with each defect takes you to the search results page.

Prerequisites

In addition to the converged appliance requirements, the following items are required to view application health and performance data on CA Performance Center:

- .NET or Java agents are monitoring business services, business transactions, and business transaction components.
- Defects and incidents are available for the monitored business transactions/business transaction components.
- TIM is reporting defects, incidents, and customer experience metrics (shown as RTTM on the UI) to Enterprise Manager.
- CA Performance Center Integration Pack installable component is installed on the Enterprise Manager or MOM.
- The following services are installed with the Enterprise Manager and running:
  - Introscope web services
  - CA CEM service
  - CA APM Model web services
  - Application Triage Map

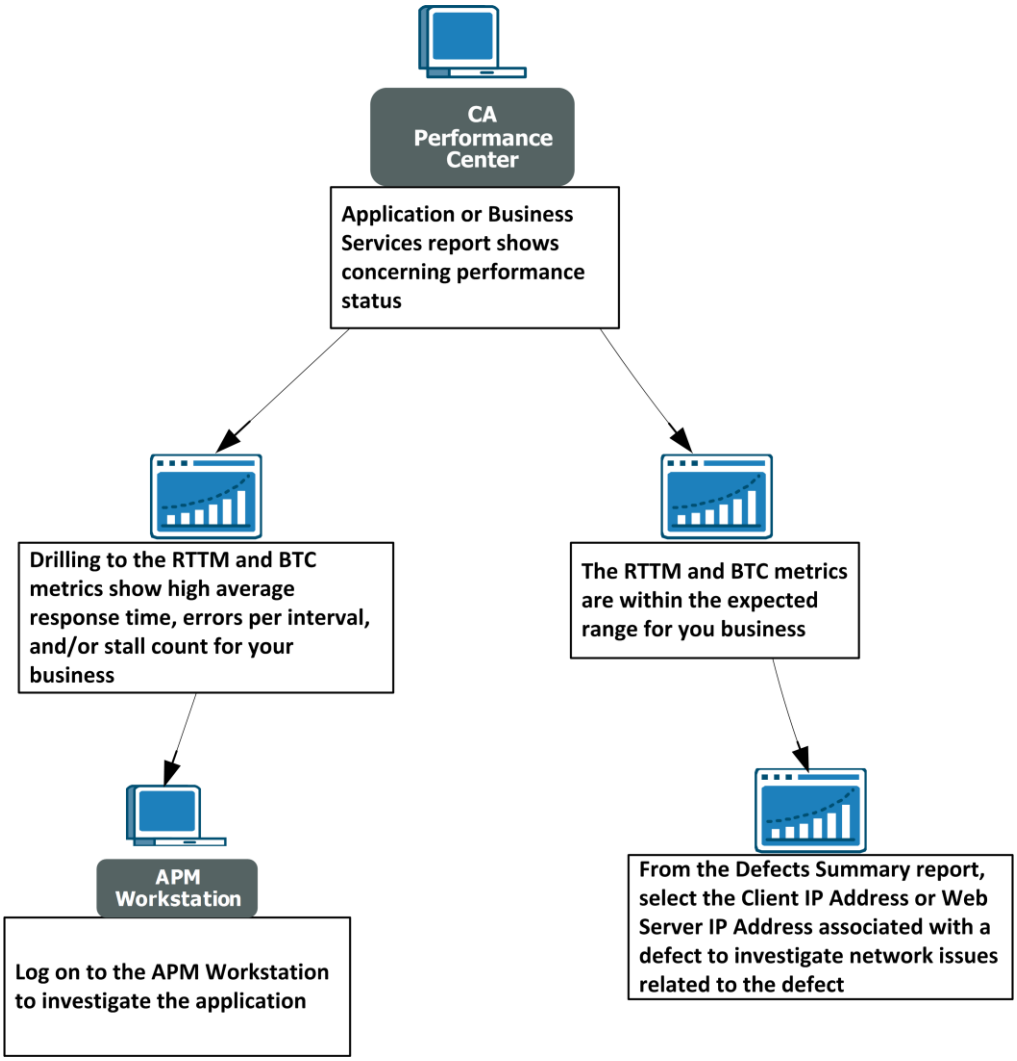
- Summary alerts are configured on the Workstation. Application triage map alerts are required to display applications, business services, and business transactions health status indicators in CA Performance Center.

How to Triage from CA Performance Center

Application data on the CA Performance Center allows support engineers to perform the following tasks:

- View health statuses of application and business services.
- Drill down to defects and more detailed metrics.
- If the application metrics show the expected performance for your business, you can immediately view the web server or client with the defect you are triaging.

The following diagram shows a possible triaging scenario.



APM - Applications Summary Dashboard

The APM - Applications Summary dashboard page shows the health status of business applications. Access this dashboard from the Application Health menu.

CA APM monitors performance and health of Java, J2EE, and .NET applications. The front-ends are referred to as applications.

A business application is a software program that automates a business service. CA APM monitors web transactions, which are the product of web applications. A business application is part of the transaction hierarchy.

The Application Status view on this dashboard shows the following information:

Applications

Lists the CA APM monitored applications. Only applications with defined business transaction components are displayed in this report. Select one to see the associated business services.

Status

The health status of the application for the specified time range. Use this information to determine which application requires further investigation. The colors represent:

- White - No data because Enterprise Manager is not responding (no metric value)
- Gray - No data (metric value: 0)
- Green - Good (metric value: 1)
- Yellow - Caution (metric value: 2)
- Red - Danger (metric value: 3)

APM - Business Services Summary

The APM - Business Services Summary dashboard page shows the health status of business services for the selected application. Drill down from an application or navigate directly from the Application Health menu to access this dashboard.

A CA APM business service is a group of business transactions. Measurements are aggregated to this level in the transaction hierarchy.

The Business Service Status view on this dashboard shows the following information:

Business Services

Lists the business services for the selected application. Select one to see the associated business transactions.

Status

The health status of the business service for the specified time range. Use this information to determine which business service requires further investigation. The colors represent:

- White - No data because Enterprise Manager is not responding (no metric value)
- Gray - No data (metric value: 0)
- Green - Good (metric value: 1)
- Yellow - Caution (metric value: 2)
- Red - Danger (metric value: 3)

APM - Business Transactions Summary

The Business Transactions Summary report shows the health status of business transactions for the selected business service. Drill down from the APM - Applications Summary or APM - Business Services Summary to view this report.

The term business transaction describes a sequence of back-to-back, computer-generated transactions. They do not include user-generated transactions that can add varying client behavior (think time) to the transaction. A business transaction consists of an identifying transaction and a number of other related transactions which can be executed in order. Transactions can be designated as included, cache-able, or both. Business transactions are defined in the CEM console.

Note: For more information on defining and creating business transactions, see the *CA APM Transaction Definition Guide*.

The Business Transaction Status view on this report shows the following information:

Business Transactions

Lists the business transactions for the selected service. Select one to see the associated customer experience metrics (shown as RTTM on the UI) and Business Transaction Component (BTC) metrics and incidents.

Status

The health status of the business transactions for the specified time range. Use this information to determine which business transaction requires further investigation. The colors represent:

- White - No data because Enterprise Manager is not responding (no metric value)
- Gray - No data (metric value: 0)
- Green - Good (metric value: 1)
- Yellow - Caution (metric value: 2)
- Red - Danger (metric value: 3)

APM - Metrics and Incidents Summary

The APM - Metrics and Incidents Summary report shows Business Transaction Component metrics and customer experience metrics (shown as RTTM on the UI) for the selected business transaction. CA APM agents report Business Transaction Component metrics per business transaction. These metrics are sometimes called Blame metrics. TIMs collect customer experience metrics per business transaction and send them to the Enterprise Manager.

Business Transaction Component Metrics

CA APM agent reports five Business Transaction Component metrics per business transaction. These five metrics are sometimes referred to as BLAME metrics. The BTC views include the following metrics:

Average Response Time (ms)

Response Time is the time it takes for a request to complete; this provides a basic measurement of application response speed. Therefore:

- Low response times are desirable.
- High response times suggest a problem.

The Average Response Time metric averages the response times of all requests that were completed during an interval.

Note: The *count* for Average Response Time is identical to the value of Responses Per Interval.

Responses Per Interval

Responses Per Interval reflects number of invocations finished that interval; it is a measure of data throughput and thus of application performance. Generally:

- A high number is desirable.
- A low number is undesirable.
- Of course, an unexpected spike in responses could indicate overuse of the external system, such as a denial of service attack on a website.

Concurrent Invocations

Invocations are requests handled by the application and its various parts; concurrent invocations are the requests being handled at a given time.

Introscope calculates the Concurrent Invocations metric by counting the number of requests which were still in flight (that is, which were still being handled) at the end of a particular interval.

- A low Concurrent Invocations value is desirable.
- A high Concurrent Invocations value suggests a problem.

Errors Per Interval

Errors are the number of exceptions reported by JVM and HTTP error codes. Examples of errors include:

- a 404 Page Not Found status reported by the HTTP server
- a SQL exception
- a Java exception

Obviously, a low error count is desirable.

Stall Count

Stalled requests are those which have not completed within a specified time threshold. If a request is counted as stalled, that does not mean it is hung and will never be completed, but that its execution exceeded the stall threshold.

- A low count is desirable.
- A high count is undesirable.

The default stall threshold is 30 seconds.

Information on stall events is stored in the Transaction Events database.

Customer Experience Metrics

TIMs collect customer experience metrics (shown as RTTM on the UI) per business transaction and send them to the Enterprise Manager. If more than one TIM monitors the same business transaction, these metrics are aggregated on the Enterprise Manager.

Customer experience includes the following metrics:

Average Response Time (ms)

For each interval, the average time it took to execute the business transaction, in milliseconds.

Total Defects Per Interval

Number of defects for all defect types for a business transaction, aggregated across TIMs.

Total Transactions Per Interval

Total number of transactions for the business transaction, aggregated across TIMs, per interval.

Defect Types

Customer experience metrics (sometimes shown as RTTM on the product UI) are grouped into several defect types. They can appear under any of these types, which are the default names of defects before users customize them.

Defect metrics will be collected for each defect type associated with the business transaction, including user-named transactions -- such as "Slow time for *<BT_Name>".*

Following are the default values for each defect type, where s = second.

Slow Time

Transaction Time > 5.000 s

Fast Time

Transaction Time < 0.005 s

High Throughput

Throughput > 100.0KB / s

Low Throughput

Throughput < 1.0KB/ s

Large Size

Transaction Size > 100.0KB

Small Size

Transaction Size < 0.1KB

Missing Transaction

Component Timeout = 10.000 s

How Customer Experience Metrics are Calculated

Customer experience transaction metrics are calculated using Javascript calculators on the Enterprise Manager which is collecting metrics from the TIM.

NOTE: Aggregated metrics will be calculated only on a collector Enterprise Manager with a running TIM Collection Service and BTstats processor. These calculations are not run on a MOM Enterprise Manager.

Incident Details

The Incident Details view shows incidents and related information for the selected business transaction.

A CA APM *incident* represents a group of defects that are tracked based on the transaction type and defect type. Incidents represent business-affecting problems that have impacted enough end users that the business must act to correct the problem.

This Incident Details view shows the following information:

Incident ID

Identification number for each incident. Select one to see the associated defects.

Incident Name

Name of the incident

Business Services

The associated business service for the incident

Business Transactions

The associated business transaction for the incident

Status

The status of the incident. Open means that the incident has *not* been resolved. Closed means that the incident has been resolved.

Business Impact

The business impact is the measure that a defect or an incident has on the business.

CEM console assigns a business impact to each incoming defect, based on the defect associated with the business transaction, defect type, and user.

The business impact of a defect is calculated as follows:

Business transaction weight * defect type weight * user weight

For example, if the following impact level is assigned to each value:

business transaction weight = 4

defect type weight = 4

user weight = 4

Then 4 * 4 * 4 = 64

The business impact is 64.

This impact level …	Is assigned this weight …
Minimum	1
Very low	2
Low	3
Medium	4
High	5
Critical	6
Trigger immediately	7

Users

The number of affected end users for the incident within the specified time frame

User Groups

The number of affected user groups for the incident within the specified time frame.

In CA APM, a user group allows you to configure settings for a collection of (monitored) users. You do not need to configure the settings for each individual user separately. User groups can be defined so you can easily identify (monitored) user populations that are likely be experiencing problems. A user belongs to only one user group.

Defects

The number of defects for the incident within the specified time frame.

A defect is the failure of a transaction to conform to customer expectations and transaction specifications. Defects are categorized as behavioral and response defects.

A defect is a single transaction opportunity that failed. If a transaction does not meet multiple specifications, then multiple defects are generated (for example, slow time and missing components).

First Occurrence

The date/time of the first occurrence of this incident, independent of the defined time frame

Last Occurrence

The date/time of the last occurrence of this incident within the specified time frame

Defects Summary Report

The APM - Defects Summary report shows the last ten defects and their related details for the selected incident.

A defect is the failure of a transaction to conform to customer expectations and transaction specifications. Defects are categorized as behavioral and response defects. If a transaction does not meet multiple specifications, then multiple defects are generated (for example, slow time and missing components).

The Defects Summary report shows the following information:

Defect ID

Identification number for each defect

Defect Name

Name associated with the defect

Business Services

The associated business service for the defect

Business Transaction

The associated business transaction for the defect

Date and Time

Date and time the defect occurred

Value

The baseline value at which if greater than or equal to, CA APM considers the transaction defective. You can configure this baseline throughput value that triggers the defect from the following CEM console page:

Administration, Business Services, (a business service), (a business transaction), Business Transaction Specifications

Business Impact

The business impact is the measure that a defect or an incident has on the business.

CEM console assigns a business impact to each incoming defect, based on the defect associated with the business transaction, defect type, and user.

The business impact of a defect is calculated as follows:

Business transaction weight * defect type weight * user weight

For example, if the following impact level is assigned to each value:

business transaction weight = 4

defect type weight = 4

user weight = 4

Then 4 * 4 * 4 = 64

The business impact is 64.

This impact level …	Is assigned this weight …
Minimum	1
Very low	2
Low	3
Medium	4
High	5
Critical	6
Trigger immediately	7

Login Name

The login name of the associated end user for the defect

User Group

Name of the affected user group for the defect

In CA APM, a user group allows you to configure settings for a collection of (monitored) users. You do not need to configure the settings for each individual user separately. User groups can be defined so you can easily identify (monitored) user populations that are likely be experiencing problems. A user belongs to only one user group.

Client IP Address

The client IP address of the end user affected by the defect

Click to access more detailed information about the client. You are directed to the search results page on CA Performance Center for this client IP address.

Web Server IP Address

The IP address of the requesting web server associated with the defect

Click to access more detailed information about the web server. You are directed to the search results page on CA Performance Center for this web server IP address.

Web Server MAC Address

The hardware address of the network card for the server associated with the defect

Metric Values

The metric values corresponding to the colored status indicators are heuristic metrics.

The values for heuristic metrics are 1, 2 or 3:

- A value of 1 indicates that the current state of the key performance indicator appears normal.

  For example, if the application's overall response time usually varies between 600ms and 1000ms and the current value is 835ms, the response-time heuristic metric reports a 1.

- A value of 2 this indicates that the current state of the heuristic's key performance indicator is outside of normal.

  For example, if the application's CPU is usually between 30% and 60% and the current value is 75%, the heuristic value might be two.

- A value of 3 indicates that the current state of the heuristic's key performance indicator is outside of normal to a large degree.

  For example, if an application typically has no stalls or occasionally has one stall but suddenly, the application's database stops responding to requests. The number of stalls might increase to a comparably high number such as ten. In that situation, the stall heuristic for the application would report a value of 3.

By defining alerts in terms of the heuristic metrics rather than fixed thresholds, the work of determining normal values for key performance indicators shifts from the APM administrator to APM itself.

Configure More Information on Network Status Information Dashboard

The More Information buttons take you to the CA Performance Center (specifically the Network Overview and Servers Overview dashboards). Links to these pages require a one-time configuration for each button. Configuring the More Information button for the worst ten client networks enables access to the Network Overview Dashboard on CA Performance Center. Configuring the button for the worst ten client servers enables access to the Servers Overview Dashboard on CA Performance Center.

Follow these steps:

1. On the Workstation Console, select Dashboard and Edit Dashboard.

   The Editor view of the Network Status Information dashboard appears.

2. Right-click the More Information button and select Ungroup.

3. Right-click directly the More Information text and select Object Links...

   The Object Links window appears.

4. Click Edit.

   The Edit Object Link window appears.

5. Verify that the Web Link radio button is selected.

6. In the URL text box, replace *<hostname>* with the name of your CA Performance Center server.

   Note: The URL defaults to accessing NetQoS Performance Center. To access CA Performance Center, change the default so it includes your CA Performance Center port number (typically 8181) and the new address.

   To access additional network information in CA Performance Center, replace:
   `http://<hostname>/npc/default.aspx?pg=6001&mn=6001`

   with
   `http://<hostname>:CA Portal/pc/desktop/?pg=2000009&mn=3`

   To access additional server information in CA Performance Center, replace:
   `http://<hostname>/npc/default.aspx?pg=7006&mn=6003`

   with
   `http://<hostname>:CA Portal/pc/desktop/?pg=2000010&mn=3`

7. Click OK on both the Edit Object Link and Object Links windows.

8. Select File, Save on the Editor view of your report.

9. Close the Editor view.

   You and all subsequent users of the Network Status Information dashboard can now directly access the associated overview reports in CA Performance Center.

Chapter 6: Troubleshooting

This section contains the following topics:

CA APM Application Data Not Available

Symptom:

After selecting the application-related reports (Business Services Summary or Applications Summary), I do not see any CA APM data in CA Performance Center.

Solution:

Verify the following:

- You have installed CA Performance Center Integration Pack (see page 44) on the Enterprise Manager or MOM.
- You have started the APM-CAPC service (see page 46).
- You have imported the APM views (see page 46) into CA Performance Center.
- You have registered APM as a data source (see page 47) in CA Performance Center.
- You have added the APM dashboards (see page 48) to the Application Health menu in CA Performance Center.
- You have created application triage map alerts (see page 41).

TIM Stops Working

Symptom:

The TIM installed on the Multi-Port Monitor has stopped functioning properly. For example, it has stopped recording and generating statistics. Additionally, I see "skip old packets" messages in the TIM log.

Solution:

When Tim is installed on Multi-Port Monitor, the NapaTech card on Multi-Port Monitor marks the packet arrival time using the time on that card. If the system time on the Multi-Port Monitor and the NapaTech card time are different, then TIM can stop functioning properly.

Two possible use cases exist. Determine which use case applies to your situation.

1. TIM processing can sometimes lag behind the packet files from the Multi-Port Monitor. For example, if TIM is stopped and restarted or the Multi-Port Monitor is generating packet files faster than TIM can consume. Confirm TIM lag time by performing the following tasks:

   a. Confirm that the NapaTech card time synchronizes with your system time on Multi-Port Monitor.

   b. Look at the Multi-Port Monitor System Status page and verifying that it does not display a warning message.

   If you have confirmed these two scenarios, then nothing is wrong with TIM. TIM does not process packet files that are older than 15 minutes (this default value can be changed). After it skips these old packet files, TIM resumes normal processing. TIM simply needs time to catch up with the Multi-Port Monitor generated files.

2. Compare the NapaTech card time to that of your system time on Multi-Port Monitor. Use the following command from the terminal to see the NapaTech card time:

   ```
   /opt/napatech/bin/TimeConfig  -cmd time_get
   ```

   Use the following command from the terminal to see the system time on Multi-Port Monitor:

   ```
   date
   ```

   If the two times are different and the Multi-Port Monitor System Status page displays a warning message, then look at the times on the NapaTech card and Network Time Protocol (NTP) server.

   Select the time zone at the following website to get NTP time:

   ```
   http://www.time.gov/
   ```

   Consider the following scenarios and determine which one applies to your situation.

   Scenario 1

   Conditions

   - The Napatech card time is **vastly** different from the NTP time (more than 15 minutes).
   - The system time on Multi-Port Monitor is slightly different from the NTP time (less than 5 seconds).

Actions

- Synchronize the NapaTech time to the system clock by running the following command:
  `/opt/NetQoS/scripts/syncNapatechClock`
- If the NapaTech time is different from the system time on Multi-Port Monitor by **less** than 5 minutes, then the NapaTech driver OS synchronization gradually adjusts the NapaTech clock. If the NapaTech time is different from the system time on Multi-Port Monitor by **more** than 5 minutes, then the NapaTech time synchronizes with the system time on the Multi-Port Monitor immediately.

Scenario 2

Conditions

- The NapaTech card time is slightly different from the NTP time.
- The system time on Multi-Port Monitor and CEM console time is vastly different from the NTP time.

Actions

- Adjust the CEM console time to synchronize with the NTP time.
- Wait and verify that the system time on Multi-Port Monitor is set and is also synchronized with the NTP time.
- Confirm that the ntpd process on Multi-Port Monitor is running. If it is not running, start it.

  The ntpd process can stop automatically when the system time on the Multi-Port Monitor is different from the NTP time by more than 1000 seconds.

Scenario 3

Conditions

- The NapaTech card time is **vastly** different from the NTP time.
- The system time on the Multi-Port Monitor and CEM console time are also **vastly** different from the NTP time.

Actions

- Adjust the CEM console time to synchronize with the NTP time.
- Wait and verify that the system time on Multi-Port Monitor is set and is also synchronized with the NTP time.
- Confirm that the ntpd process on Multi-Port Monitor is running. If it is not running, start it.
- Synchronize the NapaTech time to the system clock by running the following command:
  `/opt/NetQoS/scripts/syncNapatechClock`

Infrastructure Data not Available on CEM Console

Symptom:

Looking at defect details in which I know there should be associated network infrastructure information, I do not see this information.

Solution:

Verify that you have configured the following correctly:

- The Multi-Port Monitor Enabled check-box on the CEM console UI (Monitors, Multi-Port Monitor machine) is enabled to initiate the web service call to the Multi-Port Monitor for the TCP data.
- The defect was generated more than 5 minutes ago. There can be a delay of up to 5 minutes before the network health data is available in the Multi-Port Monitor database. If the defect was generated less than 5 minutes ago, wait a few minutes and then refresh the browser page.

More Information Buttons on Workstation Do Not Work

Symptom:

I cannot connect directly to CA Performance Center from the Network Status Information dashboard on CA APM Workstation. The More Information buttons on this dashboard do not work.

Solution:

The More Information buttons take you to the CA Performance Center (specifically the Network Overview and Servers Overview reports). Links to these reports require a one-time configuration for each button.

Index

S

T

U

V