CA Application Performance Management

Catalyst Connector Guide

Release 2.2

CA Technologies Product References

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.

Contents

Chapter 1: Overview

This chapter introduces the CA APM Catalyst Connector.

This section contains the following topics:

About This Guide

This guide describes how to install and configure the CA APM Catalyst Connector.

CA Catalyst connectors expose data to CA Service Operations Insight (CA SOI) for visualization, analysis, and management in a heterogeneous context.

This guide contains information specific to the CA APM Catalyst Connector. For more information about CA Catalyst connectors and the CA Catalyst infrastructure that applies to all connectors and connector integrations see the documentation distributed with CA SOI.

For known issues related to this specific connector, see the CA APM Catalyst Connector ReadMe file distributed with the connector package.

Terminology

The following list contains concepts and terms that are useful for integrating a CA Catalyst connector with CA SOI or other products for the first time:

Connectors

Connectors are the links from products that consume connector data to external products. Each connector retrieves information from its integrated product and transmits the information through the connector framework to the consuming product for visualization and analysis. Connectors can also invoke operations in their integrated product (such as object creation). CA Catalyst connectors use a unified connector framework to enable integration with multiple consuming products.

USM

The *Unified Service Model* (USM) is a schema of common object types and properties to which data from all connectors is converted. The USM schema allows data from all products to be analyzed in a common interface with identical formatting.

Configuration Items (CIs)

Configuration items (CIs) are representations of IT elements managed by a domain manager. Each CI belongs to a *type* (defined in the USM schema), such as Computer System, Database, Process, and Relationship. Services are composed of CIs, and you can define relationships between CIs in services.

Connectors transform managed objects from integrated products to adhere to the USM schema and transform the objects into CIs.

Services

Services are representations of discrete business functions that contain configuration items managed by multiple domains. For example, the Trading Business Service can have available Business Transactions like Balances, Transaction Summary, Login, Options Trading and Place Order. In addition, it will have several Transaction Contexts of type Applications: Reporting Service, Authentication Service, Trade Service, Order Engine, Reporting Engine and Authentication Engine. All the Software Components (Database and Web Service) discovered by the CA APM Agent(Running Software running on a Computer System) are related to these Transaction Contexts.

You can do the following in using products such as CA SOI:

- Detect the root cause of service degradation quickly and navigate into the appropriate product to resolve problems
- Model services based on CIs or imported existing service models from integrated products to construct a comprehensive, service-centric model of your enterprise

CA Service Operations Insight

CA Service Operations Insight (CA SOI) helps overcome the challenges by unifying the health and availability information from your domain management tools and aligning with your IT services.

Alerts

Alerts are the CA SOI mechanism for reporting fault conditions and service degradation. An alert is associated with a corresponding CI, and associated alert severities determine CI condition and, ultimately, service impact. *Service alerts* are conditions generated by CA SOI based on analysis of a modeled service. Service alerts result when the condition of one or more CIs combine to impact the overall quality or risk level associated with the service.

Outbound from connector operations

Outbound operations allow a connector to get data from domain managers to use products such as CA Catalyst and CA SOI. All connectors support outbound operations from connector.

Inbound to connector operations

Inbound to connector operations invoke changes in the domain manager data store as a result of changes to the data in the consuming product. For example, CI reconciliation in CA Catalyst can change the values of CI properties. Connectors that support inbound operations can then make that change in the source domain manager so that the data matches the reconciled data. If a CI is deleted in a domain manager that CA Catalyst defines as a source of truth, connectors that support inbound operations delete the CI in other domain managers with a record of that CI.

Unified Connector Framework (UCF)

The subsystem that houses the code to read, transform, and feed the MDR and JMS client.

Entity

Other elements that do not conform to the strict definition of CI. Because, CI has a strict ITIL connotation and does not have the same meaning to all. The inclusion of the term entity applies to other elements within the USM that are not strictly a configuration item. Examples include policy, relationships, KPIs, and other CIs.

CA APM

The *CA APM* solution provides 24x7, end-to-end monitoring and management of all transactions to identify, triage, prioritize, and resolve problems before they affect your end users and your business. CA APM lets you proactively monitor and manage your increasingly complex web application services environment today and as you grow. The solution provides real-time detailed data that helps you to:

- Quickly understand and address problems before customers are impacted.
- Meet service level agreements.
- Provide the online experience that your customers expect.

CA Introscope® Workstation

The *Workstation* is a thick client user interface to the metrics, alerts, and other elements that the Enterprise Manager provides.

WebView

WebView is a thin-client, slimmed-down version of the information that the Workstation provides.

CA CEM

CA CEM is the Customer Experience Manager web interface. CA CEM shows transactions, incidents, and other data collected about website user experience by the Transaction Impact Monitor (TIM) component of the Enterprise Manager.

CA APM Catalyst Connector

CA APM provides performance monitoring and incident triage capabilities across various application platforms. The central component of CA APM is the Enterprise Manager. The CA APM Catalyst Connector enables CA SOI to connect with the CA APM Enterprise Manager, thus providing visibility within CA SOI to the configuration items and information that CA APM collects. The CA APM Catalyst Connector displays CA APM data in the form of transactional and behavioral configuration items and alerts from CA Introscope® and CA CEM. CA SOI users are able to visualize the applications that are hosted within their own infrastructure on the management console.

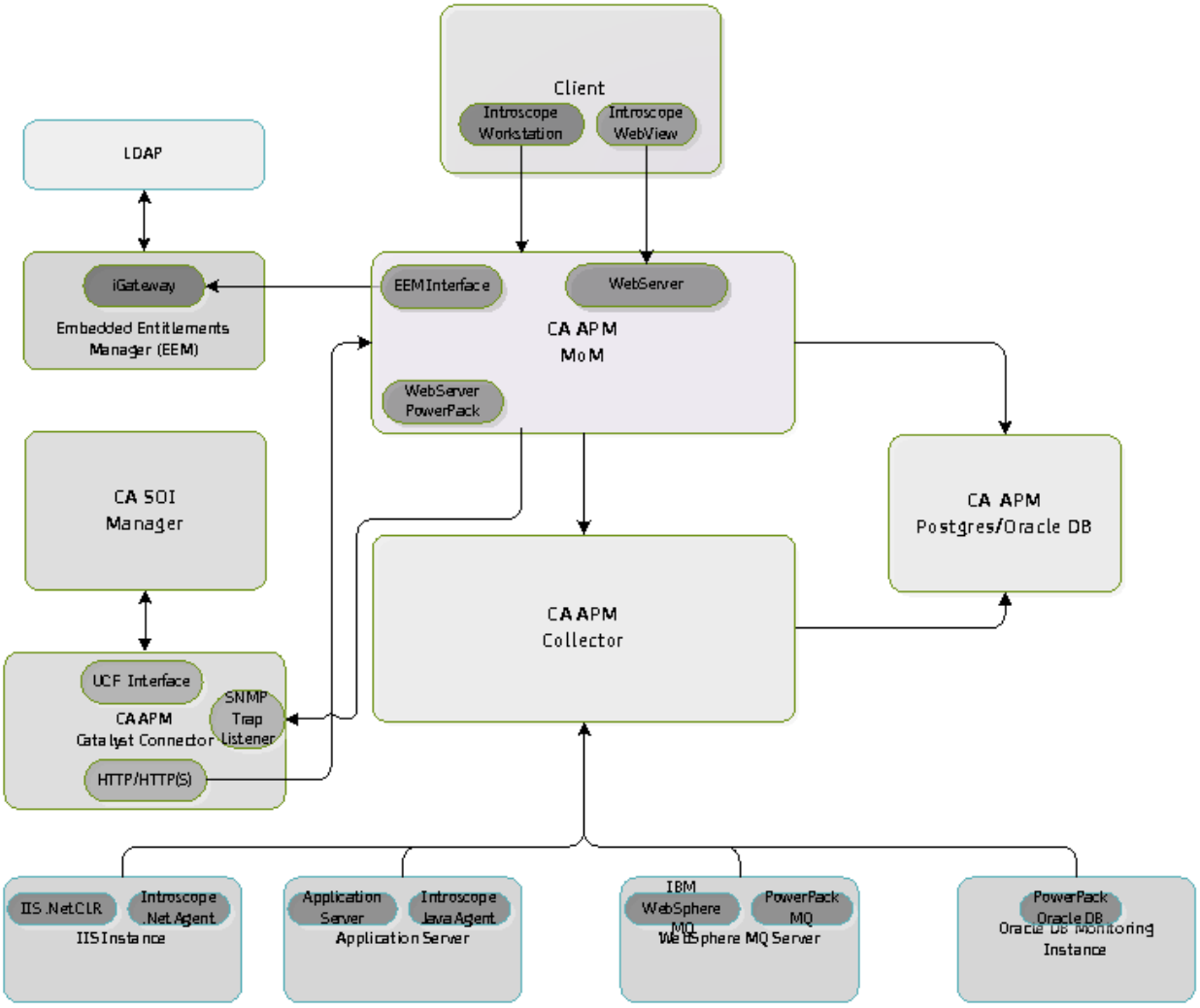
The Enterprise Manager code provides correlation properties and ability to update or delete CA APM objects. The delete feature provides access to deleted objects in the APM database. This feature provides information about the deleted CIs on CA APM to Catalyst, so that CA APM-related USM objects are synchronized.

Note: The connector does not support updates of CA APM CI attributes.

Deployment Scenario Without TIM

This deployment scenario shows a CA APM environment with basic CA Introscope® 9.x agents, extensions, and no Transaction Impact Monitor (TIM) in the environment:

The following diagram illustrates this deployment scenario:



In one case, various components send data as follows:

- The CA APM 9.x agents monitoring the Java application server send basic agent data to the CA APM collector and Application Triage Map data.
- The .NET agents monitoring the IIS instances send basic agent data to the CA APM collector.
- The IBM WebSphere MQ extension (PowerPack) agents send data to the CA APM collector.
- The Oracle DB extension (PowerPack) agents send data to the CA APM collector.

A CA APM TIM does not exist in the environment and no Business Transactions have been recorded using Agent Recording.

After you install CA APM Catalyst Connector, the connector creates the following SOI CIs:

- Running Software CIs on startup for the CA APM 9.x agents and .NET agents. The connector creates Computer System CIs for the hosts on which these agents are running.
- Running Software CIs and the associated Computer System CIs on startup for the extension (PowerPack) agents. This result occurs only if the non9XJavaOrDotNETAgents flag is set to True.

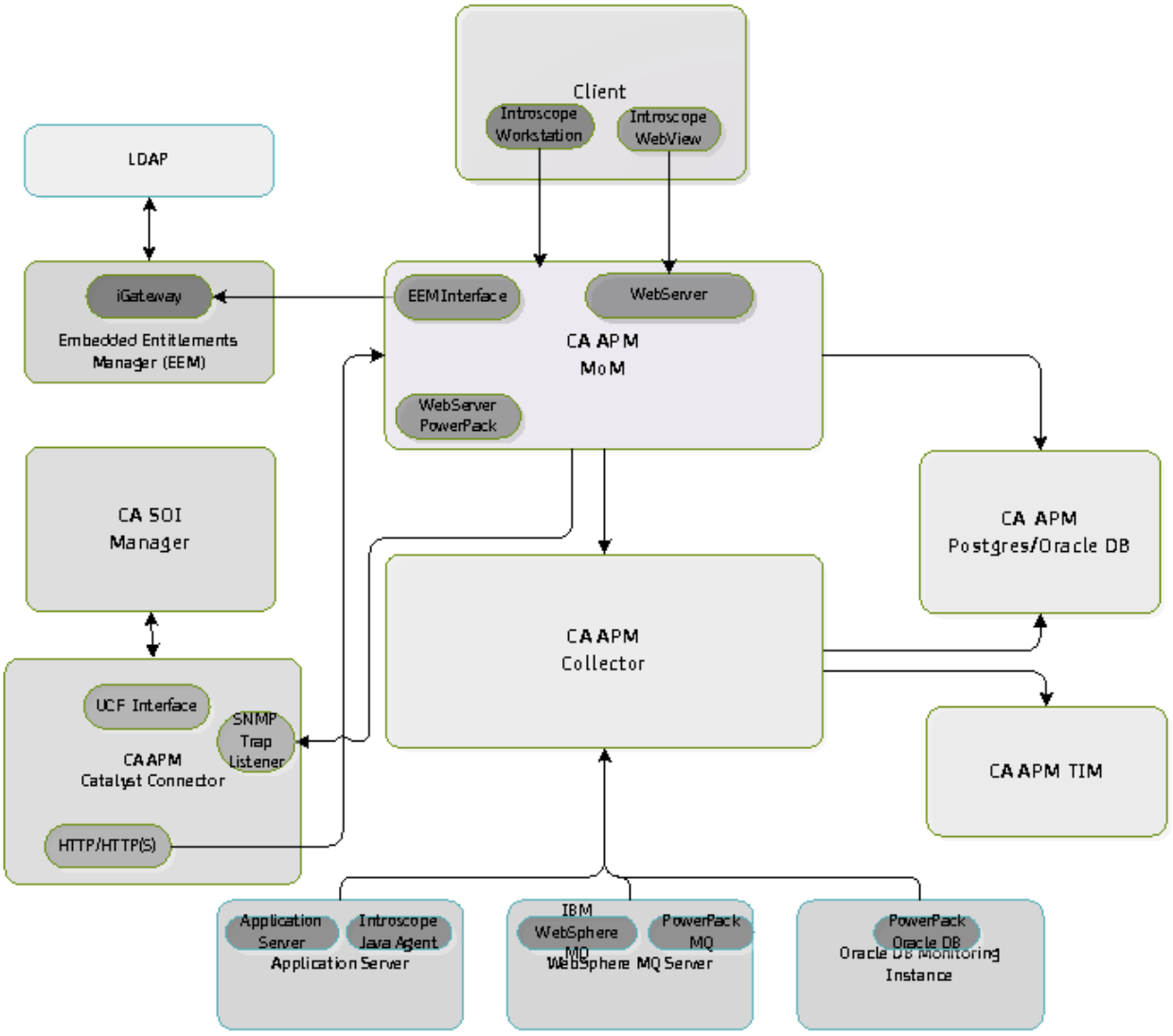
In another case, the various components send data as in the first case except Business Transactions have been recorded using Agent Recording. In this case, the connector creates the following *additional* SOI CIs:

- Service CIs, Business Transaction CIs, and Transaction Context CIs.
- If the EMGetAllCIs option is set to Yes and the ServiceImportMode value is TxTriage, the connector also creates corresponding Software Component CIs for backends in the Application Triage Map.

Deployment Scenario With TIM

This deployment scenario shows a CA APM environment with basic CA Introscope® 9.x agents, extensions, and a Transaction Impact Monitor (TIM) in the environment.

The following diagram illustrates this deployment scenario:



Various components send data as follows:

- The CA APM 9.x agents monitoring the Java application server send basic agent data to the CA APM collector and Application Triage Map data.
- The .NET agents monitoring the IIS instances send basic agent data to the CA APM collector.
- The IBM WebSphere MQ extension (PowerPack) agents send data to the CA APM collector.
- The Oracle DB extension (PowerPack) agents send data to the CA APM collector.

A CA APM TIM exists in the environment and Business Transactions have been recorded and promoted to Business Services from the TESS interface.

The connector creates the following SOI CIs after you install CA APM Catalyst Connector:

- Running Software CIs on startup for the CA APM 9.x agents and .NET agents. The connector creates Computer System CIs for the hosts on which these agents are running.
- Running Software CIs and the associated Computer System CIs on startup for the extension (PowerPack) agents. This result occurs only if the non9XJavaOrDotNETAgents flag is set to True.
- Service CIs, Business Transaction CIs, and Transaction Context CIs.
- If the EMGetAllCIs option is set to Yes and the ServiceImportMode value is TxTriage, the connector also creates corresponding Software Component CIs for backends in the Application Triage Map.

Chapter 2: Installation

This chapter includes installation prerequisites and instructions for installing the CA APM Catalyst Connector.

This section contains the following topics:

Environment Support

The CA APM Catalyst Connector supports CA Catalyst 2.5 and the following versions of CA SSA/SOI:

- CA Spectrum Service Assurance (CA SSA) 2.5
- CA Service Operations Insight (CA SOI) 3.0
- CA Service Operations Insight (CA SOI) 3.1
- CA Service Operations Insight (CA SOI) 3.2

All CA SSA/SOI Service Packs for these versions are supported.

The CA APM Catalyst Connector supports the following versions of CA APM:

- CA APM 8.x

  Note: In CA APM 8.x you cannot use the complete CA APM Service Model, or Alerts for CA CEM. You can get metrics-based alerts for CA Introscope®. These alerts are not associated with any service. The alerts are associated with Running Software (JVM) CIs, which are created on connector startup.

- CA APM 9.0 through 9.5

Note: For more information about the various CA APM elements and how they operate, see the CA APM documentation.

The CA APM Catalyst Connector supports installation on the following operating systems:

- Microsoft Windows Server 2003 (x86) SP1, SP2
- Microsoft Windows Server 2003 (x64) SP1, SP2
- Microsoft Windows Server 2003 R2 (x86)

- Microsoft Windows Server 2003 R2 (x64)
- Microsoft Windows Server 2008 (x86) SP1, SP2
- Microsoft Windows Server 2008 (x64) SP1, SP2
- Microsoft Windows Server 2008 R2

How to Perform Prerequisite Tasks

Before you begin the installation, perform prerequisite tasks.

Follow these steps:

1. Install the appropriate patches for your implementation:
   - For CA SSA 2.5 with CA APM (see page 16)
   - For CA SOI 3.0 with CA APM (see page 17)
   - For CA Introscope® (see page 18)
2. Verify installation considerations (see page 18).
3. Configure the obsolete time property (see page 22).

Note: For information about CA APM Catalyst Connector support, see the *CA APM Compatibility Guide*.

Install Patches for CA SSA 2.5 with CA APM

You install patches before you can integrate CA SSA 2.5 with CA APM.

Follow these steps:

1. Copy your CA SSA 2.5 DVD to a local drive or mapped network share. This location is referred as CA SSA media.
2. Download the following patches from CA Support, Download Center, Published Solutions, Quick Search:
   - RO25028 - WIN-CATALYST INTEGRATION MERGE MODULES
   - RO26302 - WIN-SSA MISSING ALERTS FROM APM
3. Install RO26302 (WIN-SSA MISSING ALERTS FROM APM).
   a. Extract RO26302.zip to a temporary directory.
   b. Launch RO26302.exe.
4. Extract RO25028.zip (if necessary) and Connector_APM.zip to the same folder, and then launch Connector_APM.exe.

Install Patches for CA SOI 3.0 with CA APM

You install patches before you can integrate CA SOI 3.0 with CA APM.

Follow these steps:

1. Copy your CA SOI 3.0 DVD to a local drive or mapped network share. This location is referred as CA SOI media.
2. Download the following patches from CA Support, Download Center, Published Solutions, Quick Search:
   - RO56291

     Note: Install this patch after the connector installation if you experience the following conditions:

     - The CA APM Catalyst Connector is not receiving alerts.
     - The CA APM Catalyst Connector log file does not include logging information to indicate that the APM Trap Handler was started, for example:

     ```
     " APMTrapHandler: startIncidentThread starting when thread not null")
     ```

   - RO42435

     Extract RO42435.zip (if necessary) and Connector_APM.zip to the same folder, and then launch Connector_APM.exe.

Install Patches for CA SOI 3.1 with CA APM

You install patches before you can integrate CA SOI 3.1 with CA APM.

Follow these steps:

1. Copy your CA SOI 3.1 DVD to a local drive or mapped network share. This location is referred to as CA SOI media.
2. Create the Merge_Modules folder in the Connector installer.
3. Copy IntegrationServices.iam.zip from the installation image in the Disk1\SOI folder.

   Note: For information about obtaining the image, see the CA SOI 3.1 documentation or downloads from CA Support.
4. Extract the zip file to the same folder.
5. Verify installation considerations (see page 18) and follow the prerequisites before you install the connector.

Install Patches for CA SOI 3.2 with CA APM

You install patches before you can integrate CA SOI 3.2 with CA APM.

Follow these steps:

1. Copy your CA SOI 3.2 DVD to a local drive or mapped network share. This location is referred to as CA SOI media.
2. Create the Merge_Modules folder in the Connector installer.
3. Copy IntegrationServices.iam.zip from the installation image in the Disk1\SOI folder.

   Note: For information about obtaining the image, see the CA SOI 3.2 documentation or downloads from CA Support.
4. Extract the zip file to the same folder.
5. Verify installation considerations (see page 18) and follow the prerequisites before you install the connector.

Install Patches for CA APM

For CA APM 9.0.6.1 and earlier versions, download and install the following patch:

RO28562 - WIN - CA APM SNMP ALERT ACTION PLUGIN

More information:

Install the SNMP Alert Action Plugin (see page 23)
Create and Configure the SNMP Alert Action (see page 24)

Verify Installation Considerations

Before you begin the installation, identify the following information, which you enter during the installation process.

Note: The configuration steps are applicable to CA SSA 2.5, CA SOI 3.0, or CA SOI 3.1 depending upon the version you have installed on your computer.

Follow these steps:

1. Identify the following information for the Integration Services Configuration dialog:

   Manager host

   Specifies the name or IP address of the CA SOI or CA SSA host server depending on version.

   Note: The installer does not accept an IPv6 address. For IPv6 hosts, type the name of the host. For IPv4 hosts, enter either the host name or the IPv4 address.

   ActiveMQ port

   Specifies the port number on the CA SOI or CA SSA host server to use.

   SA Admin

   Specifies the userid of the CA SOI or CA SSA administrator account you want the CA APM Catalyst Connector to use.

   Password

   Specifies the password for the CA SOI or CA SSA administrator account.

   Connector name

   Specifies the name of this instance of the CA APM Catalyst Connector. By default, the installer populates this field with a name based on the server you are installing the connector from.

2. Identify the following information for the APM Connector Configuration dialog:

   APM Enterprise Manager Hostname

   Specifies the host name or IP address where the Enterprise Manager is installed. Either a standalone Enterprise Manager or clustered Manager of Managers (MOM) Enterprise Manager.

   Note: The installer does not accept an IPv6 address. For IPv6 hosts, type the name of the host. For IPv4 hosts, enter either the host name or the IPv4 address.

   APM Enterprise Manager User

   Defines the username for a user of the Enterprise Manager. The User must have the same privileges as the Admin user.

   The default user for connecting to the Enterprise Manager is Admin.

   APM Enterprise Manager Password

   Specifies the password for the Enterprise Manager user, if one exists. Default installations of Enterprise Manager use a blank password.

   APM Protocol

   Specifies the protocol to use for the connection. Must be either http or https.

APM Enterprise Manager Web Server Port

Specifies the port that you want the connection to use. The default is port 8081, which the Enterprise Manager uses for a web interface or any other port you dedicate to the connection.

3. Identify the following information for the APM SNMP Trap Configuration dialog:

APM MOM EM IP Address

Specifies the IP address of the Enterprise Manager where the SNMP Alert Action Plug-in is installed. The address can be a standalone Enterprise Manager or a clustered Manager of Managers (MOM) Enterprise Manager.

Default: Null

APM Connector IP Address

Configures the SNMP Bind Address to listen for the SNMP trap containing CA Introscope® alert data. The IP address of the host where the connector is installed.

Default: Null

APM SNMP Community

Defines the SNMP community relationship between an SNMP server system and the client systems. This string acts like a password to control the access of the client to the server.

Default: public

APM Connector SNMP Trap Listener Port

Configures the SNMP Port to listen for the SNMP trap sending CA Introscope® alert data.

Default: 162

Check for CA APM Data

Valid for: CA APM 9.x agents

Verify that the CA APM database is populated with the required CA CEM and CA Introscope® data that can be obtained through the CA APM Catalyst Connector.

Verify that the following data is present in the APM Database:

Look for data in tables beginning with the apm_ prefix. You can run the following SQL queries to check if there is any data in the APM tables:

```
select * from apm_vertex;
select * from apm_agent;
select * from apm_edge;
select * from apm_owner;
```

Check for Application Triage Map Tuning

We recommend that customers tune their environment according to application usage before they start the process of installing the CA APM Catalyst Connector.

When the introscope.apm.data.preserving.time value is not low enough to manage the Application Triage Map data in your environment, an error that resembles the following one may appear:

```
connector.ApmConnector - getEdges::Exception:
com.wily.apm.model.webservices.exception.ApmWebServicesException:
java.util.concurrent.ExecutionException:
com.wily.apm.model.data.exception.TooManyRowsRetrievedException
```

Tune the property introscope.apm.data.preserving.time correctly for your application usage. We recommend a 60-day value, however, base this value on your understanding of the application usage in the environment.

Note: For more information about setting this property, see the topic "Configure Application Triage Map Data Pruning" in the *CA APM Configuration and Administration Guide.*

If other circumstances prevent you from setting the value low enough, you can increase the value for introscope.apm.query.max.results property. Set this value in the APMEnterpriseManager.properties file to prevent this exception.

Configure the Agent for ComputerSystem CIs

Valid only for: 8.x agents

Agent properties let you control the behavior and operation of the agent and customize settings to suit your environment. You can configure an agent running on a host to reconcile with other computer systems. The agent then reports fully qualified hostnames to the Enterprise Manager. These names appear in CA Catalyst and CA SOI as ComputerSystem CIs based on the fully qualified hostnames.

Follow these steps:

1. Navigate to the IntroscopeAgent.profile file location in your CA APM implementation.

   Note: When you install an agent, the agent profile is installed in the <*Agent_Home*>/wily/core/config directory.

2. Open the IntroscopeAgent.profile file in a text editor.
3. Set the following property to true:

   ```
   introscope.agent.display.hostName.as.fqdn=true
   ```

4. Save and close the file.

Configure the Obsolete Time Property

The default value of the property introscope.apm.data.obsolete.time in the IntroscopeEnterpriseManager.properties file is 300 days. For the CA APM to CA APM/CA APM Catalyst Connector integration, before you start the connector, change the default value of this property to a lower value.

Follow these steps:

1. Shut down the CA Enterprise Manager.
2. Open the IntroscopeEnterpriseManager.properties file in the <*EM_Home*>/config directory.
3. Verify that the introscope.apm.data.obsolete.time property is uncommented. Specify HOURS or DAYS; 24 hours or 1 day is the minimum. We recommend 15 days. This value ensures that CA APM objects, which have not been used by a CA APM agent recently, are deleted from CA APM Catalyst Connector/CA SOI.
4. Save and close the IntroscopeEnterpriseManager.properties file.
5. Restart the Enterprise Manager.

   The obsolete time property is configured.

6. View the message logs in the <*EM_Home*>/logs directory. For example:

   ```
   10/19/13 12:02:13 PM EST [INFO] [Manager] [ The APM Data  property:
   introscope.apm.data.obsolete.timeset to value : 15 DAYS]
   ```

Note: For more information about this property, see the *CA APM Administration and Configuration Guide*.

How to Create and Configure an SNMP Alert Action

If you want to get CA Introscope® alert data, you use the SNMP Alert Action Plug-in. This plug-in enables the CA APM Catalyst Connector to pass CA Introscope® alert data to CA SOI.

Important! Metrics-based alerts are CA Introscope® alerts created through the Management Module editor and not through the triage map. Summary alerts for metrics-based alerts are not supported.

You configure Management Module objects so that the SNMP Alert Action Plug-in sends CA Introscope® data to CA APM Catalyst Connector. Plugin configuration settings specify which alerts forward data to the CA APM Catalyst Connector. You configure these settings in CA Introscope® Management Module objects as follows:

1. Create one or more alerts.

   Your SNMP Alert Action requires at least one alert to reference.

2. Create an SNMP Alert action which references the alerts you created.

Your SNMP Alert Action requires at least one alert to reference. An CA Introscope® alert is simply a holder for Caution and Danger threshold settings.

Important! When creating an alert for your SNMP Alert Action to reference, verify that Notify by individual metric is selected. If you do not select this option, then false or misleading alerts are raised in CA SOI. For the procedure about creating an alert and management modules, see the *CA APM Workstation User Guide,* in the CA APM documentation.

Install the SNMP Alert Action Plugin

Valid for: CA APM 9.0.6.1 and earlier

Before you begin:

Obtain the SNMP Alert Action Plugin download archive:

- Windows: SNMPAlertActionPlugins.zip
- UNIX: SNMPAlertActionPlugins.tar
- RO28562 - WIN - CA APM SNMP ALERT ACTION PLUGIN

Contact CA Support to obtain the SNMP Alert Action Plugin.

Note: In the following instructions, *<EM_Home>* describes the Enterprise Manager home directory. On Windows, this directory is typically C:\Program Files\CA APM\Introscope *<Version>.*

Follow these steps:

1. Stop Enterprise Manager.

2. Uncompress the archive, ensuring the extracted jar files in ext and lib subdirectories are readable by the user under which Enterprise Manager runs.
   - Windows: Unzip SNMPAlertActionPlugins.zip to *<EM_Home>*.
   - UNIX: Untar SNMPAlertActionPlugins.tar to *<EM_Home>:*

     ```
     tar xvf SNMPAlertActionPlugins.tar
     ```
3. Restart Enterprise Manager.

Create and Configure the SNMP Alert Action

You can create an SNMP Alert action that references the alert you have created.

Follow these steps:

1. Identify the Management Module that is the source of the CA Introscope® alerts you want to transform to Alert CIs.
2. Create an SNMP Alert action:
   a. From the Elements menu, select Elements, New Action, New SNMP Alert Action
   b. Type a name for the new action.
   c. Confirm that the correct Management Module is shown. If not, select the correct one from the list.
   d. Select the Active check box.
3. Configure the following information in the SNMP Destination section:

   Host IP

   Defines the IP address of the host server where the connector is installed.

   Note: Only IPv4 is supported.

   Trap Port

   Defines the SNMP Trap port that is configured on the connector host server.

   Default: 162.

   Community

   Defines the SNMP community string relationship between an SNMP server system and the client systems. This string acts like a password to control the client access to the server.

   Use the same value as the EMSNMPCommunity property configured during the CA APM configuration.

4. Configure the following information in the Introscope WebView section:

   Protocol

   Specifies the connection protocol. Select one of the following protocols:

   - http
   - https

   Host IP

   Defines the IP address of the host server on which the WebView component is installed. In a cluster environment, this setting applies to the MOM Enterprise Manager.

   EM/MOM

   Defines the IP address of an Enterprise Manager or the MOM Enterprise Manager in a cluster environment.

   - Only IPv4 is supported.
   - The Host IP address must be set to the same as the Enterprise Manager IP address.

   Port

   Defines the WebView port number.

   Default: 8080.

   Management Module

   Specifies the name of the Management Module where the action resides.

   Dashboard Name

   Specifies the name of the CA Introscope® dashboard where the alert appears.

5. Click Apply.

   Important! When you configure an alert, add the SNMP Alert Action created with the appropriate Caution and the Danger thresholds. Select the Whenever Severity Changes option for the Trigger Alert Notification from the drop-down list in the Alert configuration.

6. Click Test to verify the communication between the Enterprise Manager and the APM connector. A message similar to the following one appears in the APM_Connector.log file at <*catalyst_container_home*>container\data\log.

   ```
   2012-06-28 07:59:41,389 INFO
   [10.130.113.7_60045_KickProcessIncomingMessage_15] connector.APMTrapHandler -
   Test trap received - discarded.
   ```

   The SNMP action alert configuration is set.

Uninstall the SNMP Action Alert Plugin

The SNMP Alert Action Plug-in is included in CA APM beginning with version 9.0.6.2. Before upgrading from CA APM 9.0.6.1 or earlier to CA APM 9.0.6.2 or later, uninstall the plug-in .jar files. When you perform the upgrade, the installer automatically installs the necessary files for the plug-in.

Follow these steps:

1. Stop Enterprise Manager.
2. Delete the following files:
   - *<EM_Home>*/ext/SNMPAlertActionEM.jar
   - *<EM_Home>*/ext/SNMPAlertActionWS.jar
   - *<EM_Home>*/lib/snmp6_1.jar
3. Restart Enterprise Manager.

Metric-Based Alerts in CA APM

For metric-based alerts in CA APM, we recommend the following setup:

Turn on SQL normalization for any CA Introscope® agent that uses an SNMP alert action to send alerts for SQL metrics to CA APM Catalyst Connector/CA SOI.

Configure the SNMP destination (see page 26) if you want the initial state of metric-based alerts to be available on the CA APM Catalyst Connector.

Configure Triage Map Alerts in CA APM

Triage map alerts are sent to the CA APM Catalyst connector from SNMP traps through an SNMP Triage Map Alert Action handler. This action occurs when you configure triage map alerts.

Note: Do not create metric-based alerts for the triage map through the Management Module editor.

Follow these steps:

1. Configure the SNMP destination in the IntroscopeEnterpriseManager.properties file to send the triage map alerts, for example:

```
######################################################################
# SNMP Configuration for Triage Map Alerts for SSA/Catalyst
#
# ====================================================================
# This needs to be set to the ip address of the SSA/Catalyst connector
# where the triage map SNMP traps will be sent.
introscope.apm.catalyst.triagemapalert.snmp.destination.host.ip=
# This needs to be set to the SNMP port where the triage map SNMP traps
# will be sent. Default value is 162.
introscope.apm.catalyst.triagemapalert.snmp.destination.trap.port=162
# This needs to be set to the SNMP community string. Default value is public.
introscope.apm.catalyst.triagemapalert.snmp.community=public
# This needs to be set to the trigger type desired for SNMP trap notifications.
Default
# value is numeric equivalent of trigger Whenever Severity Changes.
introscope.apm.catalyst.triagemapalert.snmp.trigger=3
```

   Note: For the initial state of metric-based alerts, the host address must match the host address for the SNMP Alert Action for the connector.

2. Select the Broadcast to Catalyst check box in the triage map alert.

   The SNMP Listener on the connector listens for the traps and processes them separately depending on whether the alert is for:

   - A Business Transaction CI.
   - A Transaction Context CI.

   Note: If the same CA APM owner is in two or more CA APM Business Services, the owner is translated into unique Transaction Contexts for each service in CA SOI. However any alerts that are associated with such an owner are generated for each Transaction Context, regardless of which Business Service it originated from.

Install the CA APM Catalyst Connector

Follow these steps:

1. Double-click the installer executable, Connector_APM.exe.

   If all the prerequisites are met, the Introduction page of the installer opens.

   Note: If the Missing Common Installation Files error appears, verify that you have installed the CA SSA 2.5 and CA SOI 3.0 patches (see page 16).

2. Click Next.

   The License Agreement page opens.

3. Scroll to the bottom of the agreement before the "I accept" button is enabled.
4. Select "I accept the terms of the License Agreement." and click Next.
5. Specify the installation folder. You can:
   - Accept the default: C:\Program Files\CA\SSA or C:\Program Files\CA\SOI.
   - Type a path of your choice.
   - Click the Choose... button to select another path on your network.
6. Click Next, when the correct path is entered.
7. In the Integration Services Configuration dialog, provide information that lets the CA APM Catalyst Connector to connect to your CA SOI server.

   If you already have installed an instance of the CA SOI framework, the installer does not display the Integration Services Dialog. Go to the next step.

   In addition to the connection parameters (see page 18):

   a. If you want the installer to verify the connection with the CA SOI host server on clicking Next, select the Verify connection check box. This check box is selected by default.

   b. When you enter host names, the installer does not accept an IPv6 address. For IPv6 hosts, type the name of the host. For IPv4 hosts, enter either the host name or the IPv4 address.

   c. If you want the CA APM Catalyst Connector to use DNS resolution, select the check box labeled "Use DNS for name resolution." This check box is selected by default.

   d. The installer populates the field with a default name based on the server you are installing from. If you erase or replace this name, you can click the Default button to repopulate this field with the default name.
8. Click Next, when you have finished entering values and changes in the dialog.
9. In the APM Connector Configuration dialog (see page 18) provide information that lets CA SOI connect to the APM Enterprise Manager.
10. Click Next.

    If CA SOI is not already installed, then the installer creates a Windows service, CA SAM Integration Services.

    Note: If you want your computer to start this service at the completion of the installation process, verify that the Start Services option is selected.

    If CA SOI is already installed, the CA SAM Integration Services exists.
11. Click Next.

The installer displays the information that you entered and tells you how much disk space is required for the installation.

12. Click Install, if the values are correct.

    The installation begins.

    When the installation is complete, it displays the Install Complete dialog. This dialog gives you the filename and path to the installation log.

13. Click Done.

Verify the Installation

After the installation completes successfully, you verify the installation.

Follow these steps:

1. Browse to the C:\Program Files\CA\log directory.
2. Review the install logs and verify that no error messages have been reported.

```
APM_Install_2.5.x.x.log:
…
#Catalyst APM Connector - Service Startup
#---------------------------------------
StartServices=true

Summary
-------

Installation: Successful.

164 Successes
0 Warnings
0 NonFatalErrors
0 FatalErrors
```

3. Investigate any errors. Browse to the <*SOI_HOME*>\logs and view the APM_Connector.log file.

Uninstall the CA APM Catalyst Connector

You can uninstall the CA APM Catalyst Connector when it is no longer required.

Follow these steps:

1. From the Start menu, select Programs > CA > Service Assurance Manager > Uninstall APM Connector.

   The connector uninstalls and the Uninstall Complete page lists the result of the process, including any errors that occurred.

2. When the uninstall process completes, click OK.

Note: Uninstalling the CA APM Catalyst Connector does not remove it from the CA SOI UI.

More information:

Remove the CA APM Catalyst Connector (see page 30)

Remove the CA APM Catalyst Connector

Follow these steps:

1. Open the CA SOI Administration user interface and click the Administration tab.

   The Administration page opens.

2. Expand Connector Configuration and the connector server name, and click the entry for the CA APM Catalyst Connector.

   A page opens for the CA APM Catalyst Connector.

3. Verify that the connector status is Offline.

4. Click Remove Connector.

   A message prompts you to confirm that you want to delete the connector database entry.

5. Click OK.

   The CA APM Catalyst Connector registration is removed from the CA SOI database. The connector name is removed from the tree on the Administration tab and all other interfaces.

Note: Relationships are not sent at startup. The CA APM Catalyst Connector only sends CIs that CA SOI or CA SSA use. You can restore the previous behavior to send relationships at startup and the unused CIs. This behavior causes connector processing large data sets and runs out of memory. Moving to a 64-bit JVM (if supported by the operating system) resolves this problem, but the Catalyst Connector Framework is not certified for 64-bit JVM.

The connector entry takes a considerable time before it is removed from the CA SOI Administration UI. If it is not removed after waiting for some time, try to remove it again and look at the CA SOI logs for any potential problem.

More information:

Uninstall the CA APM Catalyst Connector (see page 30)

Upgrade the CA APM Catalyst Connector

To use the latest features and enhancements, upgrade the CA APM Catalyst Connector.

Follow these steps:

1. Uninstall (see page 30) the CA APM Catalyst Connector.
2. Install (see page 27) the latest CA APM Catalyst Connector version.

Chapter 3: Configuring the CA APM Catalyst Connector

After installing the CA APM Catalyst Connector, you can change the connector properties you defined during installation and edit other properties to refine connector behavior or adjust to changes in the integrated product.

This section contains the following topics:

Configure the CA APM Catalyst Connector (see page 33)

Configure the CA APM Catalyst Connector

You can configure the CA APM Catalyst Connector to change any default values for the parameters that were set during the installation of the connector.

Follow these steps:

1. Open the CA SOI Administration user interface and click the Administration tab.

   Note: For more information about accessing the CA SOI interfaces, see the *CA Service Operations Insight Administration Guide*.

   The Administration page opens.

2. Expand Connector Configuration and the connector server name, and click the entry for the CA APM Catalyst Connector.

   A page opens for editing the configuration settings.

3. In the Connection Details table, change any of the following properties and click Save.

   These properties are set in the Connector APM_<*EM_Host*>.xml file in <*Connector_Home*>\ resources\Configurations\.

   Important! Do not change any properties in the Connection Details table other than the ones listed here.

   ServiceImportMode

   Defines the type of service import. Review the service models (see page 63) before you set an option.

   Default value: MacOnly

Possible values:

App

Designates the frontend which the alert was generated on. In this mode, TransactionContext is filtered so only data of the type Application is accepted.

MacOnly

Specifies that the Transaction Context (that is, frontend application) does not appear.

TxTriage

Displays additional Software Component CIs, which are backends in CA APM of type sockets and databases.

Note: Set the EMGetAllCIs property to Yes to enable this service mode. If you do not set EMGetAllCIs to Yes, the service model appears the same as in MacOnly mode.

EMCIPollInterval

Specifies the interval at which the CA APM Enterprise Manager is polled. The polling checks if any CIs have been added, updated, or deleted in CA APM. The default value is 60 minutes. The maximum value is 35790 minutes. Any illegal values are ignored and the default is used.

Note: The EMCIPollInterval value is set in minutes and the EMIncidentPollInterval value is set in seconds. Verify that the EMCIPollInterval value is never lower than the EMIncidentPollInterval value. For example, when the EMIncidentPollInterval value uses the default of 300 seconds (5 minutes), the EMCIPollInterval value must be 5 minutes at a minimum.

EMConnectionPassword

Specifies the password for the CA APM Enterprise Manager user.

Note: A default installation of CA APM does not require a password for the Enterprise Manager, in which case this field is left blank.

EMConnectionUser

Specifies the userid for an Enterprise Manager user. The CA APM Catalyst Connector uses the CA Introscope® security model web services to access CA APM. For authentication and communication to the CA Introscope® Enterprise Manager, the CA APM Catalyst Connector uses the Enterprise Manager username and password.

If you are not using the default userid of “Admin” for the Enterprise Manager connection, ensure that the user specified in EMConnectionUser has Admin permissions. Also ensure that this user belongs to the Administrator group.

If the Enterprise Manager is enabled with CA EEM (CA EEM) and Business Application policies are defined in CA EEM, ensure that the EMConnectionUser belongs to these two administrator groups:

- Administrator
- CEM System Administrator

Ensure that the EMConnectionUser has the necessary permissions before starting the connector in each of these cases.

Note: For information about configuring CA EEM authentication, see the *CA APM Security Guide* and the *CA APM Installation and Upgrade Guide*.

EMHost

Specifies the host name or IP address where the CA APM Enterprise Manager is installed.

EMWebserverProtocol

Specifies the protocol to use for the connection. The protocol must be either http or https.

EMWebserverPort

Specifies the port to use for the connection. The Enterprise Manager uses this port for a web interface. You can use another port you that you dedicate to the connection.

Default: 8081

EMIncidentPollInterval

Specifies the interval in seconds at which the Enterprise Manager is polled to check for new CA CEM incidents. The default value is 300 seconds (5 minutes).

EMSNMPTrapPort

Configures the SNMP Port to listen for the SNMP trap sending CA Introscope® alert data.

Default value: 162

EMSNMPBindAddress

Configures the SNMP Bind Address to listen for the SNMP trap containing CA Introscope® alert data. The IP address of the host where the connector is installed.

Default: Null

EMSNMPHostIPAddress

Specifies the IP address of the Enterprise Manager where the SNMP Alert Action Plug-in is installed.

Default: Null

EMSNMPCommunity

Specifies the SNMP community string that defines the relationship between an SNMP server system and the client systems. This string acts like a password to control the client access to the server.

Default value: public

EMGetAllCIs

Specifies that backends in CA APM of type sockets and databases are sent to CA APM Catalyst Connector/CA SOI as Software Component CIs.

Note: The Software Component CIs are shown in a SOI Service Model only when the TxTriage mode is configured on the connector.

Default: No

APMUseAgentFqhn

Specifies if the CA APM Catalyst Connector uses the fully qualified host name from the apm_agent table.

Default: No

non9XJavaOrDotNETAgents

Specifies how the connector looks for agents that are not CA APM 9.x Java or .NET agents. For CA Introscope® 8.x agents, EPAgents, or any agents from extensions that report to the Enterprise Manager in the environment, set this flag to True. A True value causes the connector to report these agents as Running Software CIs to CA APM Catalyst Connector/CA SOI.

Default: False

4. If you want to obtain CA Introscope® alert data, configure CA Introscope® alert settings before stopping and restarting the Connector.
5. Click Stop, and then click Start.

   The connector restarts and the configuration changes apply.

   Note: To avoid connector issues, do not perform rapid stops and starts of the connector.

   The default value for the getRelationshipsAtStartup property is 0. This value reduces initial start-up time for the connector and has no impact on the data that is viewed in the CA SOI console. If you want to see the relationships at startup, then set the getRelationshipsAtStartup property value to 1.

Configure Connector Instances

You can configure more than one instance of the CA APM Catalyst Connector on a computer, with each instance pointing to a different Enterprise Manager host.

Follow these steps:

1. Rerun the installer from the same computer.
2. Supply new CA APM connection information.

   Two configuration files, APMConnector_<*EM_Host*>.xml and APMConnector_<*EM_Hostname*>.conf are created. *EM_Host* is the name of the new Enterprise Manager to which you are connecting.

Security Error Occurs When the Enterprise Manager is Using HTTPS

Symptom:

The Enterprise Manager webserver is running in HTTPS mode. A security error occurs when the connector initializes.

Solution:

1. Go to the bin folder of the jre (for example, C:\Program Files\CA\SOI\jre-32\bin) that the CA SOI installation uses.
2. Run the following command:

   C:\Program Files\CA\SOI\jre-32\bin>.\keytool -keystore ..\lib\security\cacerts -import -trustcacerts -storepass changeit -noprompt -alias CAWilyCert -file ..\..\resources\APMConnector.cer

   Note: The APMConnector.cer security certificate is in the resources folder of the CA APM Catalyst Connector installation.

Manually Configure Multiple Connector Instances

You can modify existing instances of the CA APM.

Note: Multiple CA APM connectors can be installed within the same SSA/SOI framework. Entries in the APM_Connector.log file are interleaved between the connectors. When you configure multiple connectors, verify that each connector is listening on a different SNMP port.

Follow these steps:

1. Stop the CA SAM Integration Services service on the connector server.
2. Copy the following file and name the copy uniquely:

   <*SOI_Home*>\resources\configurations\APM_<*EM_Host*>.xml

Note: Where *<EM_Host>* is the name of the Enterprise Manager to which the connector connects.

The *<SOI_Home>*\resources\configurations directory contains two *APM_<EM_Host>*.xml files, where the host names are for different Enterprise Manager hosts.

3. Open the new *APM_<EM_Host>*.xml configuration file with a text editor.
4. Edit the following parameters in the line that begins with 'Silo':

   name

   Specifies a name using a unique string to represent your connector. For example, “CA:00001_xxx.xxx.xxx.xxx” where xxx is the IP Address of your CA APM instance. You can change it to “CA:00001_hostname” where hostname is where CA APM is running. The unique name is necessary to differentiate multiple instances running on the same server.

   state

   Specifies whether the instance is enabled or disabled, set it to *enabled.*

   MdrProduct

   Specifies the product code (CA:00001) that the connector is connecting to (CA APM in this case).

   Do not change this value.

   MdrProdInstance

   Specifies the host name where CA APM is running.

5. Edit the following parameters in the line that begins with 'ConnectionInfo':

   EMConnectionPassword

   Specifies the password for the Enterprise Manager to connect to.

   EMConnectionUser

   Specifies the userid for an Enterprise Manager user. The CA APM Catalyst Connector uses the CA Introscope® security model web services to access CA APM. For authentication and communication to the CA Introscope® Enterprise Manager, the CA APM Catalyst Connector uses the Enterprise Manager username and password.

   If you are not using the default userid of “Admin” for the Enterprise Manager connection, ensure that the user specified in EMConnectionUser has Admin permissions. Also ensure that this user belongs to the Administrator group.

If the Enterprise Manager is enabled with Embedded Entitlements Manager (CA EEM) and Business Application policies are defined in CA EEM, ensure that the EMConnectionUser belongs to these two administrator groups:

- Administrator
- CEM System Administrator

Ensure that the EMConnectionUser has the necessary permissions before starting the connector in each of these cases.

Note: For information about configuring CA EEM authentication, see the *CA APM Security Guide* and the *CA APM Installation and Upgrade Guide*.

EMHost

Specifies the host name or IP address where the Enterprise Manager is installed.

EMWebserverProtocol

Specifies the protocol to use for the connection. Must be either *http* or *https*.

EMWebserverPort

Specifies the port the Enterprise Manager uses for a web interface. Default is 8081.

RetryCount

Specifies the number of times the connector attempts to establish a connection with the Enterprise Manager web server. This value must be an integer.

RetryInterval

Specifies the time, in seconds, between attempts to establish a connection with the Enterprise Manager web server. This value must be an integer.

Host

Specifies the host name or IP address where the Enterprise Manager or MOM is installed.

Use the same value as the EMHost parameter.

Example:

```
<ConnectionInfo EMConnectionPassword="" EMConnectionUser="Admin"
EMHost="1.2.3.4" EMWebserverProtocol="http" EMWebserverPort="8081"
RetryCount="20" RetryInterval="30" host="1.2.3.4"/>
```

In this example, the connector attempts to establish a connection with the web server at the specified host for 20 times (the RetryCount). Every 30 seconds (the RetryInterval) the connector tries another 20 attempts.

EMCIPollInterval

Specifies the interval at which the CA APM Enterprise Manager is polled to check if any CIs have been added, updated, or deleted in CA APM. The default value is 60 minutes. The maximum value is 35790 minutes. Illegal values are ignored and the default is used.

EMIncidentPollInterval

Specifies the interval, in seconds, at which the Enterprise Manager is polled to check for new CA CEM incidents. The default value is 300 seconds (5 minutes).

EMSNMPTrapPort

Configures the SNMP Port to listen for the SNMP trap sending CA Introscope® alert data.

Default value: 162

EMSNMPBindAddress

Configures the SNMP Bind Address to listen for the SNMP trap containing CA Introscope® alert data. The IP address of the host where the connector is installed.

Default: Null.

EMSNMPHostIPAddress

Specifies the IP address of the Enterprise Manager where the SNMP Alert Action Plug-in is installed.

Default: Null

EMSNMPCommunity

Specifies the SNMP community string that defines the relationship between an SNMP server system and the client systems. This string acts like a password to control the clients access to the server.

Default value: public

EMGetAllCIs

Specifies that the connector sends Software Component CIs to CA Catalyst.

Set the EMGetAllCIs value to Yes if you want the connector to get the software component CIs into Catalyst.

Note: The TXTriage Service Import model in CA SOI uses these CIs. Set this flag to Yes for the TxTriage service model to work.

Default: No

APMUseAgentFqhn

Specifies that CA APM Catalyst Connector uses the fully qualified host name from the apm_agent table for CA APM 9.x agents.

Set this value to Yes if your application uses CA APM agents version 9 and later.

Defaut: No

6. If you want to get CA Introscope® alert data, then you configure CA Introscope® alert settings now, before stopping and restarting the Connector.
7. (Optional) When the password to the Enterprise Manager is encrypted, you run the Encrypt Password Utility. (see page 42)

   Note: Do not change the parameters for the LICURL (Launch-In-Context URL) entries.
8. Save and close the *APM_<EM_Host>*.xml file after making your changes and start the CA SAM Integration Services service. The new connector instance connects to the specified product instance and begins collecting information.

Manually Create a Service for Running Software CI

You can encounter the following cases where you must manually create a service in CA SOI. Then you associate the service with a Running Software CI.

- Applications without frontends

  You configure an alert before you can import the computer that the agent is running on as a Running Software CI. You can configure this alert for any metric that the agent returns.
- EPAgent

  When using an EPAgent, you must configure an alert and associate with a Running Software CI.

To obtain metrics-based alerts for CA Introscope® for any of these cases, use the CA SOI Service Modeler to create a service manually. To create a service to associate a Running Software CI, use the CA SOI interface. You manually create a service and then attach a Running Software CI to the new service.

Note: You perform this step after you configure the Catalyst Connector for APM.

The CA APM Catalyst Connector generates running Software and Alert CIs when any metrics-based alerts are sent through an SNMP trap that has appropriate configuration settings.

To create a service and attach a Runtime Software CI in CA SSA 2.5 or CA SOI 3.0, perform the following procedure.

Follow these steps:

1. Open the CA SOI Console.
2. From the File Menu, select Tools > Create New Service.
3. Locate the agent under Computer System > Running Software.
4. Right-click the new node in the tree under Running Software and select Add with subcomponents.
5. Give a name to the new service, and save.
6. Generate an alert and verify the event in the CA SOI console.

More information:

Verify that an Application Does Not Have Frontends (see page 42)

Verify that an Application Does Not Have Frontends

You can verify that an application does not have frontends.

Follow these steps:

1. Verify that your application is used.
2. Verify that your application does not have frontends:
   - In the Investigator, Overview tab, you see the message: "There are no applications on this agent."
   - In the Metric Browser tree, there is no Frontends node.
   - Your server is not listed in the APM database apm_agent table.

   If these items are all true, your application does not have frontends.

Encrypt a Password

When the CA APM Catalyst Connector must connect to an Enterprise Manager using a password, run a password encryption utility. This utility is a batch file named EncryptSAMCreds.bat.

Follow these steps:

1. Browse to the C:\Program Files\CA\<*SOI_Home*>\Tools directory.
2. Run the EncryptSAMCreds.bat file using the password as a parameter to the command. For example, if the password for the Enterprise Manager is sample_pwd, run:

   ```
   C:\Program Files\CA\SOI\Tools>EncryptSAMCreds.bat sample_pwd
   ```

   The command returns an encrypted password (for example, *EKnTt5kPbagAoWRvwKjKV7XEtsxCMGade6fjVir8IXGWt*) that you can paste into the connector configuration file.

Enable Debugging

You can enable debugging for the CA APM Catalyst Connector-specific logs.

Follow these steps:

1. Browse to the C:\Program Files\CA\SOI\resources\Configurations\log4j folder.
2. Open the CA APM log configuration file (Apm_log4j.xml) and set the logging level to TRACE:

   ```
   <logger name="com.ca.wily.apm" additivity="false">
   <level value="TRACE"/>
   <appender-ref ref="APMConnector"/>
   </logger>
   ```

3. Save and close the file.

Chapter 4: Connector and Domain Manager Interaction

This chapter discusses the type of data exchanged through the CA APM Catalyst Connector.

This section contains the following topics:

How the Connector and Product Interact

The CA APM Catalyst Connector gets information from CA APM to CA SSA 2.5, CA SOI 3.0, or CA SOI 3.1 in this way:

1. During connector start, configuration properties, which supply information about CA APM and CA SSA or CA SOI instances for connection, are initialized by the connector.
2. The SNMP Alert Action Plug-in captures data from CA Introscope® alerts and formats the data into an Alert configuration item (CI).

   Note: If you are monitoring alerts for SQL metrics, configure the CA APM agent to normalize the SQL metrics before the connector starts. For information about normalizing the SQL statements for metrics, see the *CA APM Java Agent Implementation Guide*.
3. The Connector calls to the APM web services API to discover the following lists:
   - All CIs present in the APM database.
   - Relationships (see page 50) between CIs.
   - Incidents, which the connector transforms to Alert CIs.
   - Initial states of CA Introscope® alerts, which the connector transforms to Alert CIs.
   - Relationships between software components and computer systems (the physical system on which the agent is installed) based on the DeviceDnsName field.
   - Business Services and Business Transactions that are deleted using the TESS UI.

4. The values in the ServiceImportMode are drawn from the ServiceImportMode parameter in the connector configuration file. The ServiceImportMode parameter determines how the connector filters data before sending it to CA SOI Manager.

Note: CA USM Configuration Items that are created based on CA APM objects remain in the CA Catalyst database. Objects are not deleted even when the source CA APM objects are deleted or renamed in the CA APM database.

The following CIs are imported:

Service

A Service in the CA APM context is a collection of business transactions, manually created by the user using the Transaction Recording. It is a well-defined application or service, or a set of applications or services. It is useful to a business and is managed distinctly.

Alert

An Alert indicates a detected problem in CA APM. The alert is triggered by threshold breaches in CA Introscope® metrics cause the alert, CA CEM incidents caused by defects, or breach of thresholds for entities within the Triage Map.

Business Transaction

A Business Transaction is the result of a transaction recording, which is generally a series of transactions that are meaningfully tied to one another. Example: Login, Order, and Logout.

Computer System

A Computer System is the host on which the CA APM agent is installed.

Software Component

A Vertex is the software component responsible for performing a certain operation. A software component can have a parent-child relation with another software component. From the CA Introscope® agent perspective, it is an instrumented class-method pair and analogous to a vertex or node in the AppMap dependency map. For example, a servlet, database connection, or a web service.

Note: Software Component is only imported if the parameter EMGetAllCIs, in the connector configuration file, is set to Yes.

Transaction Context

The Transaction Context or Owner is an entity describing the flow of information for an application or a transaction. A transaction context is either of type application or business transaction. A transaction context of type application defines an application that contains one of more software components. A transaction context of type business transactions provides a link between the operational or software and business views of the environment.

Running Software

Running Software is the representation of the CA APM agent. The agent runs within the application server monitoring applications and the server. Agents run on a physical or virtual host.

A process named transaction recording defines service and business transactions. The user turns on the recording feature within CA APM and asks the end user to describe the "behavior" while executing a series of transactions that are meaningfully tied to one another, for example, Login, Order, Logout. CA APM records these transactions and later lets the user bundle the recorded business transactions into a list named the service. CA APM also allows for automated recording without any explicit user interaction by using predefined templates to aggregate business transactions and bundle them into services.

When you delete business services and business transactions from the CEM Console, the corresponding CIs are also deleted from the CA Catalyst and CA SOI databases. This deletion occurs when the connector receives updates that are based on the EMCIPollInterval.

CA APM agents automatically discover Transaction Contexts, and Software Components.

Transaction Contexts and Software Component CIs are marked for being obsolete based on the introscope.apm.data.obsolete.time property in the Enterprise Manager setting. This Enterprise Manager property is set to define the time limit for objects in the APM Transaction model to be considered as obsolete. The supported time units for this property are HOURS and DAYS. 24 HOURS or 1 DAY is the minimum time that this property supports. The default value is 300 days.

More information:

How to Create and Configure an SNMP Alert Action (see page 22)
Configure Triage Map Alerts in CA APM (see page 26)

Run the Network Interface Utility

The Network Interface Utility is used to locate network interface name values for the introscope.agent.primary.net.interface.name= property.

Note: The Network Interface Utility is available for Java and .NET agents. You can configure and run this utility in CA Introscope® Agent interface but not on the CA APM Catalyst Connector.

Follow these steps:

1. Navigate to the following directory:

   <Agent_Home>\common\wily\tools directory

2. Run the Network Interface tool.

   The network interface details are displayed in a browser, if the Operating System supports it. Otherwise the network interface details in HTML form are saved in a standard XML output.

   Note: When the introscope.agent.display.hostName.as.fqdn property is set to false only short hostname is propagated to the CA APM Catalyst Connector. This breaks the connection with the other product that uses fqdn hostname.

Note: For more information about using the Network Interface Utility, see the *CA APM Java Agent Implementation Guide* or the *CA APM .NET Agent Implementation Guide*.

More information:

Configure a List of Available Networks (see page 48)

Configure a List of Available Networks

The introscope.agent.primary.net.interface.name property specifies the primary network interface name of the host computer used by the agent for the Catalyst integration. You can change the configuration of this property and the change is applied automatically.

Note: When the agent logging level is set to DEBUG, information about network interface names available for configuration appears in the log file. Alternatively, you can use the Network Interface utility to determine the primary network interface name for this property.

Follow these steps:

1. Open the default IntroscopeAgent.profile file in a text editor.
2. Locate the line: introscope.agent.primary.net.interface.name=<false|true>, and specify the name value.

   The following example shows the name format:

   ```
   introscope.agent.primary.net.interface.name=eth4
   ```

   Note: The default value is undefined. When this property is not set, the agent assigns the first available network interface as the primary interface. You can use the Network Interface utility to determine the name value for this property.

3. (Optional) Allow for multiple network addresses by specifying the subinterface number (starts at 0).

   The following example shows the subinterface number format:
   `introscope.agent.primary.net.interface.name=eth4.1`

4. Save and close the file.

   The profile is set up to use the configuration.

CA Introscope® Alerts

The information that is available for import and the configuration item (CI) to which the connector converts it depends on your version of CA APM. The Catalyst Connector selects the CA APM version automatically. The default version is CA APM 9.5.

Note: The CA APM installation must use the TIM utility so that CA CEM incidents can be associated with a business transaction and a business service.

- The ServiceImportMode parameter in the connector configuration file uses the App mode, the MacOnly mode, or the TxTriage mode. When Service Import occurs, the Service Model (see page 63) uses the mode that is configured in the CA SSA/SOI Service Modeler Topology.
- For CA APM 9.6, the following information is available:

  CA SOI enables a visual model to be displayed with the relationships between frontend applications and their backends. The backends displayed are of type sockets and databases. Thus, you can perform end to end triage from the applications layer to the system level. This data is gathered by setting the EMGetAllCIs flag to yes.

  Note: If the same backend has been discovered by multiple agents, which are associated with a single business service, then the model will display the backend discovered by each agent separately.

- For CA APM 9.1 through 9.5, the following information is available only when the connector is configured to App mode in the ServiceImportMode parameter:

  Note: For CA APM 9.6 at a minimum if TxTriage is configured, the following information will also be available:

  - Metrics-based CA Introscope® alerts which are associated with a service under Running Software CI.
  - CA CEM incidents that are associated with business transactions in the service model.
  - Business transaction-related Triage Map alerts under a business transaction and frontend Triage Map alerts associated with the Transaction Context CI Application.

- For CA APM versions later than 9.0.6 and before 9.1, the following data is available:
  - Business services and business transactions in the service model
  - CA CEM incidents are associated with a business transaction.
  - Metrics-based CA Introscope® alerts that are associated with a Running Software but are displayed in the service model.
- For CA APM 9.0.6, the business transaction in the service model is available. Also available are CA CEM incidents and metrics-based CA Introscope® alerts, which are associated with a service.
- For CA APM versions before 9.0.6, the alert information that is imported from CA APM 9.0 and 9.0.5 is converted into the Alert CI. This information has the following limitations:
  - Only metrics-based CA Introscope® alert data is imported. No alerts on business services or business transactions are imported.
  - The data is not associated with any service, but is associated with the RunningSoftware CIs.
  - CA SOI Manager is not able to display this data in a topology.

USM Data Mapping

When connectors transform CA APM data to CIs, or import services from CA APM, they normalize the classes, properties, relationships, and severities in the domain manager to adhere to the USM schema. This section lists the CA APM classes and relationships and their USM mapping.

Type Mapping

This section contains tables showing how the CA APM Catalyst Connector maps its elements to USM elements.

The product ID in USM for CA APM is “CA:00001" and this can be used across all Configuration Items (CIs).

Service Table

The following table shows how the connector maps APM Business Service elements to USM_Service elements.

APM Element, Description	CA APM Type	USM element	USM Type
Name Name of the business service	String	ServiceName from Service CI	String
ID Unique ID of the business service	Integer	MDRElementID, part of MDRID	String
CreationDate Date the business service was created	DateTime	CreationTimestamp	dateTime
UpdateDate Date the business service was last updated	DateTime	LastModTimestamp	dateTime

Business Transaction Table

The following table shows how the connector maps APM Business Transaction elements to USM_Business_Transaction elements.

APM Element, Description	CA APM Type	USM element	USM Type
Name Name of the business transaction	String	GroupName from USM:Group	String
ID Unique ID of the business transaction	Integer	MDRElementID, part of MDRID	String
CreationDate Date the business transaction was created	DateTime	CreationTimestamp	dateTime
UpdateDate Date the business transaction was last updated	DateTime	LastModTimestamp	dateTime

Software Component Table

The following table shows how the connector maps APM vertex elements to USM_Software_Component elements.

APM Element, Description	CA APM Type	USM element	USM Type
ID Sequence number which acts as a surrogate Primary Key	Integer	MDRElementID, part of MDRID	String
Name Software component name	String	ComponentName	String
Type From USM_Software_Component_Type Table Examples: WebService_Client, JDBC Client, EJB	String/ Open enum	Type referenced from usm-meta:EnumDetails enumName="SoftwareComponentTypeEnum	String
Parent_ID ID of the Parent SoftwareComponent	Integer	SoftwareComponent IsComposedOf SoftwareComponent	relationship
Abstraction Level Physical or Logical	Char/Enum	isLogical is true or false	boolean
Hierarchy Level Level of Hierarchy. E.g., Class, Class-Method, Process, JVM, and other method. Hierarchy Level allows you to understand the zoom level for the software component - JVM, Java Class, and Java Method.	Open Enum	HierarchyLevel from usm-meta:EnumDetails enumName="HierarchyLevelEnum	String

APM Element, Description	CA APM Type	USM element	USM Type
Properties List of name value pares used for special display of a particular node. These properties can be used to correlate with physical parts of USM – for example, components of the JDBC connection string could be in properties Example: jdbc:host1133:4435:DBname:DBInstance	Name Value Pairs list	NameValuePairs	String
Creation Date When created	Datetime	Entity: CreationTimestamp	dateTime
Update Date When updated	Datetime	LastModTimestamp	dateTime
FullyQualifiedHostName Fully qualified physical host name	String	DeviceDnsname	String

Transaction Context Table

The following table shows how the connector maps CA APM owner attributes to USM_Transaction_Context attributes.

APM Element, Description	CA APM Type	USM element	USM Type
ID Unique ID of the owner	Integer	MDRElementID, part of MDRID	String
Type Type of owner. For example, “Web Application”	String/Enum	Type from usm-meta:EnumDetails enumName="ContextTypeEnum	String
Name Owner name	String	ContextName	String
Creation Date When created	Datetime	Entity: CreationTimestamp	dateTime

APM Element, Description	CA APM Type	USM element	USM Type
Update Date When updated	Datetime	Entity: LastModTimestamp	dateTime
User_name Who updated	String	n/a -- dropped	n/a

RunningSoftware CI Table

The following table shows RunningSoftware CI elements and values.

APM Element, Description	CA APM Type	USM element	USM Type
“RS:”+Id (HostName_Process_Agent)	String	MDRElementID, part of MDRID	String
EM Host Name (read from the connector configuration)	String	MdrProdInstance	
LastModTimestamp (current time)	Datetime	Entity: LastModTimestamp	dateTime
"WilyUser"	String	LastModUserName	String
“ManagedApplicationContainer:CA :WilyAPM: HostName_Process_Agent"	String	InstanceName	String
“ManagedApplicationContainer”	String	TypeName	String
false	Boolean	isInMaintenance	Boolean
"CA"	String	Vendor	String
"WilyAPM"	String	ProductName	String
“HostName+ Process + Agent”	String	ProcessDistinguishingID	String
IPv4 An IPV4 device address received from the “ipv4” property in the Introscope Agent.	String	DeviceIPV4Address	String
IPv4-DomainName An IPv4 address and domain name received from the "ipv4" and "DomainName" properties in the Introscope Agent.	String	DeviceIPV4AddressWithDomain	String

APM Element, Description	CA APM Type	USM element	USM Type
IPv6 An IPV6 device address received from the “ipv6” property in the Introscope Agent.	String	DeviceIPV6Address	String
IPv6-DomainName An IPv6 address and domain name received from the "ipv6" and "DomainName" properties in the Introscope Agent and which are concatenated together in CA USM policy file.	String	DeviceIPV6AddressWithDomain	String
HostName.DomainName The host name received from the Introscope alert or from Introscope agent. A concatenation of HostName and DomainName.	String	DeviceDnsName	String
MacAddress A Mac address received from the "mac" property in the Introscope Agent.	String	DeviceMacAddress	String

ComputerSystem Table

The following table shows ComputerSystem CI elements and values.

APM Element, Description	CA APM Type	USM element	USM Type
“CS:”+Id (HostName_Process_Agent)	String	MDRElementID, part of MDRID	String
Enterprise Manager Host Name (read from the connector configuration)	String	MdrProdInstance	String
CreationTimestamp (current time - Create with a date while creating CS)	Datetime	Entity:CreationTimestamp	dateTime
LastModTimestamp (current time)	Datetime	Entity: LastModTimestamp	dateTime
Fully qualified host name of the system where the agent is installed	String	PrimaryDNSName	String
Fully qualified host name	String	InstanceName	String
Fully qualified host name	String	ComputerName	String

APM Element, Description	CA APM Type	USM element	USM Type
IPv4 An IPV4 device address received from “ipv4” property in the Introscope Agent.	String	PrimaryIPV4Address	String
IPv4-DomainName An IPv4 address and Domain name received from the "ipv4" and "DomainName" properties in the Introscope Agent.	String	PrimaryIPV4AddressWithDomain	String
IPv6 An IPV6 device address received from “ipv6” property in the Introscope Agent.	String	PrimaryIPV6Address	String
IPpv6-DomainName An IPv6 address and domain name received from the "ipv6" and "DomainName" properties in the Introscope Agent.	String	PrimaryIPV6AddressWithDomain	String
HostName.DomainName A fully qualified host name and domain name received from the "HostName" and "DomainName" properties in the Introscope Agent.	String	PrimaryDnsName	String
PrimaryMacAddress A Mac address received from the "mac" property in the Introscope Agent.	String	MacAddress	String

Alerts Mapping

Both CA Introscope® alerts and CA CEM incidents map to USM types.

CA Introscope® Metrics-Based Alerts for Running Software CI

The SNMP Alert Action Plugin creates an Alert CI from CA Introscope® alert data.

The following table shows CA APM alert elements mapped to Alert CI elements:

CA APM Element, Description	CA APM Type	USM element	USM Type
AlertName+a hash of AlertHost+AlertAgent+AlertMetric from the SNMP Trap	String	MDRElementID, part of MDRID	String
Enterprise Manager Host Name	String	MdrProdInstance	String
None **Note:** Will only be populated if the Introscope metrics-based Alert contains UrlParams.	String	UrlParams	String
OccurrenceTimestamp The time the Alert was triggered from the trap	Datetime	Entity:OccurrenceTimestamp	dateTime
ReportTimestamp Current time	Datetime	Entity:ReportTimestamp	dateTime
LastModTimestamp (current time)	Datetime	Entity: LastModTimestamp	dateTime
CA APM metric name	String	AlertType (see page 62)	String
CA APM alert severity	String	Severity (see page 62)	String
HostName_Process_Agent	String	AlertedMdrElementID	String
Obtain from the Alert message and get a summarized field: Examples: "MedRec Home Responses Per Interval" exceeded danger target of 4 “CPU Utilization Alert" opened a caution alert with a target of 8	String	Summary	String
Message from the SNMP trap if it is populated.	String	Message	String
From CA Introscope® Alert in the trap	String	MetricDetails	String

CA Introscope® Triage Map Alerts for Business Transaction CI

The following table shows CA Introscope® Triage Map Alert elements mapped to Business Transaction CI elements:

APM Element, Description	CA APM Type	USM element	USM Type
"AL:"+Id (Use a combination of "Business Transaction Name_Business TransactionId" from the SNMP trap received that contains it in AlertedComponentName_ AlertedComponentID or from owningEntityName_owningEntityId in DAlertSnapshot.)	String	MDRElementID	String
Enterprise Manager Host Name (same as value in Connector configuration)	String	MdrProdInstance	String
The Alert triggered time from the trap if SNMP trap received. Create Date in the DAlertSnapshot if the initial state of alert is received.	dateTime	OccurenceTimestamp	dateTime
'currentTime' – the time when Alert was reported to USM	dateTime	ReportTimestamp	dateTime
The rolled up summary alert is mapped as follows **Metric**: ■ Summary Alert **USM Alert Type:** ■ Risk-Performance	String	AlertType	String

APM Element, Description	CA APM Type	USM element	USM Type
From the Introscope Alert: **Alert Severity:** ■ Normal (1) ■ Caution (2) ■ Danger (3) **USM Severity Type:** ■ Normal ■ Major ■ Critical	String	Severity	String
Enterprise Manager Host Name	String	AlertedMdrProdInstance	String
"BT:" + BusinessTransactionID	String	AlertedMdrElementID	String
Content in the Rolled Up Summary message in the SNMP trap	String	Summary	String

CA Introscope® Triage Map Alerts for Transaction Context Type Application

The following table shows CA Introscope® Triage Map Alert elements mapped to Transaction Context Type Application elements:

APM Element, Description	CA APM Type	USM element	USM Type
"AL:"+Id	String	MDRElementID	String
Enterprise Manager Host Name	String	MdrProdInstance	String
The Alert triggered time from the trap if SNMP trap received.	dateTime	OccurenceTimestamp	dateTime
'currentTime' – the time when Alert was reported to USM	dateTime	ReportTimestamp	dateTime
The rolled up summary alert is mapped as follows **Metric**: ■ Summary Alert **USM Alert Type:** ■ Risk-Performance	String	AlertType	String

APM Element, Description	CA APM Type	USM element	USM Type
From the Introscope Alert: **Alert Severity:** ■ Normal (1) ■ Caution (2) ■ Danger (3) **USM Severity Type:** ■ Normal ■ Major ■ Critical	String	Severity	String
Enterprise Manager Host Name	String	AlertedMdrProdInstance	String
"TC:" + TransactionContextId	String	AlertedMdrElementID	String
Content in the Rolled Up Summary message in the SNMP trap.	String	Summary	String

CA CEM Incidents Mapping for Business Transaction CIs

The following table shows CA CEM Incident elements mapped to Alert CI elements.

APM Element, Description	CA APM Type	USM element	USM Type
Incident Snapshot	String	MDRElementID, part of MDRID	String
Enterprise Manager Host Name (same as value in Connector configuration)	String	MdrProdInstance	String
“http://host:port/wily/cem/tess/app/biz/bizEventList.html? pId=” + Id	String	UrlParams	String
StartDate	datetime	Entity:OccurrenceTimestamp	dateTime
<Current time>	datetime	Entity:ReportTimestamp	dateTime
CloseDate	datetime	Entity:RetireTimestamp	dateTime
Lookup DefectType in DefectTypeToAlertType map.	String	AlertType (see page 61)	String
ImpactName	String	Severity (see page 63)	String

APM Element, Description	CA APM Type	USM element	USM Type
Enterprise Manager Host Name (same as value in Connector configuration)	String	AlertedMdrProdInstance	String
“BT:” + BusinessTransactionId	String	AlertedMdrElementID	String
“DefectName”	String	Summary	String
Cause **Note:** Cause is usually blank unless the user has entered anything during Incident configuration from the UI.	String	Message	String
false	Boolean	IsClearable	Boolean
Status == Constants.DB_BIZ_EVENT_STATUS_CLOSED	String	IsCleared	String
Assignee	String	Assignee	String
n/a Because each CA CEM incident is related to multiple CA CEM defects, it is not possible to relate just one of those defects to an SSA/SOI incident.		RelatedIncident	
NumberOfDefects	String	RepeatCount	String
LastModified – StartDate	datetime	ElapsedTime	dateTime

CA CEM Defect Types for SSA or SOI Alerts

CA CEM defect types are mapped to SSA/SOI alert types as follows.

CA CEM Type	Defect Name	Alert Type
1	Slow Time	Quality-SlowTime
2	Fast Time	Quality-FastTime
4	Low Throughput	Quality-LowThroughput
3	High Throughput	Quality-HighThroughput
6	Small Size	Quality-SmallSize
5	Large Size	Quality-LargeSize

9	Missing Transaction	Quality-MissingTransaction
9	Missing Component	Quality-MissingComponent
10	Content Error	Quality-ContentError
11	Missing Response	Quality-MissingResponse
16	Partial Response	Quality-MissingPartialResponse
8	Unauthorized Access	Quality-UnauthorizedAccess
8	Client Request Error	Quality-ClientRequestError
8	Server Response Error	Quality-ServerResponseError
17	HTTP Response Header Parameter	Quality-TransactionHTTPResponseHeaderParameter

Notes:

- For types 8 and 9, mapping from the DefectType to the Alert type is not unique. For those types, only a second mapping table from DefectName to Alert type is used. If DefectName is not found in the second table (because it was edited in CA CEM), defects of type 8 will map to Risk, and defects of type 9 to Quality.
- Mapping is not configurable.

Alert Severity Mapping

Alert severity levels are mapped as follows:

CA APM Metric	USM Alert Type
Normal	Normal
Warning	Major
Critical	Critical

Alert Type Mapping

If the metric in the alert contains one of the following text strings, the alert is mapped as follows:

APM Metric	USM Alert Type
Average Response Time	Risk-Performance-AverageResponseTime
ResponsesPerInterval	Risk-Performance-ResponsesPerInterval
Errors Per Interval	Risk-Performance-ErrorsPerInterval

APM Metric	USM Alert Type
Stall Count	Risk-Performance-StallCount
Concurrent Invocations	Risk-Performance-ConcurrentInvocations
All other Strings	Risk-Performance

CA CEM Incident Severity Mapping

CA CEM incident severity levels are mapped as follows:

Incident Severity	USM Severity Type
Moderate	Minor
Severe	Major
Critical	Critical

Relationship Mapping

The following types of BinaryRelationships (CIs) are supported for CA APM CIs:

- Service *isComposedOf* multiple BusinessTransactions
- BusinessTransaction *HasMember* TransactionContext
- BusinessTransaction *HasMember* TransactionContext (Application)
- TransactionContext (Application) *HasMember* RunningSoftware
- RunningSoftware *isHostedBy* ComputerSystem
- TransactionContext (Application) *HasMember* SoftwareComponent
- SoftwareComponent *isImpactedBy* RunningSoftware

Service Models Supported in CA SOI

CA APM in CA SOI supports the following ServiceImportMode parameter modes for service models: App (see page 65), MacOnly (see page 66), and TxTriage (see page 68). The service model uses the mode that you configure in the CA APM Catalyst Connector configuration file for Service Import.

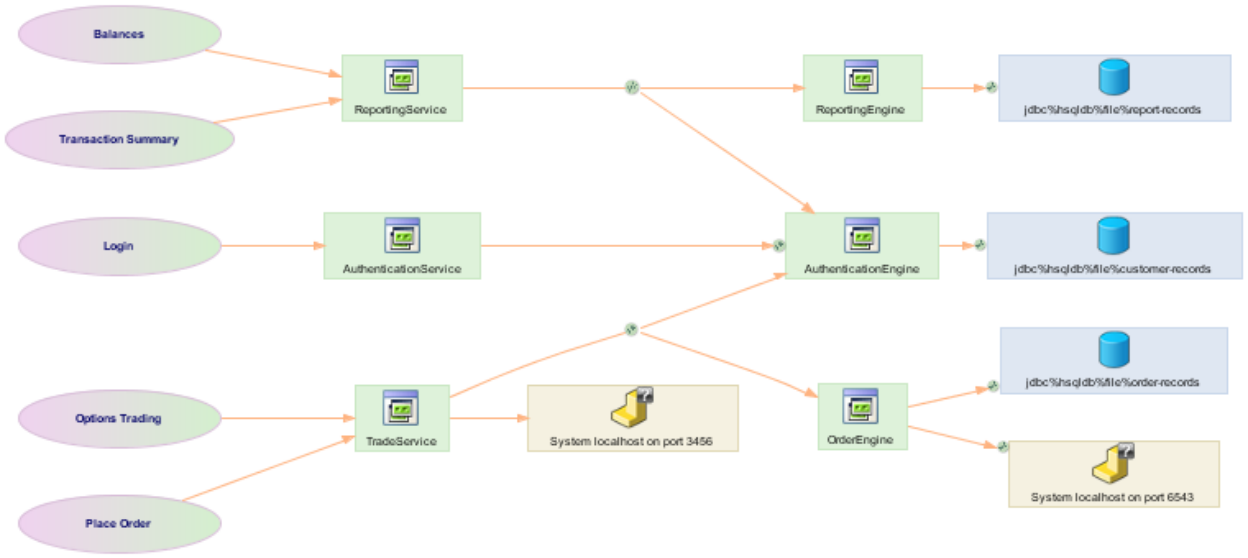
These models operate when you record a transaction using the TIM in a CA CEM environment or using agent recording. When no recording occurs, you cannot import these models into CA SOI and you must manually import CA APM supported CIs into any model you want. If no Application Triage Map data exists in the environment and only Business Services and Business Transactions are configured in CA CEM:

- The CA SOI service model shows the Business Services and Business Transactions only when you have set the MacOnly value or the App value.
- The CA SOI service model does not show anything when you have set the TxTriage value.

The connection from an application (frontend) to the Running Software (agent) shows directly in the MacOnly service model for the following setup:

- A multitiered application in an environment.
- Business Service and associated Business Transactions that denote the transaction call flow for this multitiered application.
- No backends that are associated with an application (frontend) for this multitiered application.

The following diagram shows an Application Triage Map view for the Trade Service Application (a sample application):



This diagram shows the summary of a recorded and defined Trading Business Service. This summary view is the default view within CA APM 9.x. In the diagram, you can see:

- All available Business Transactions that belong to the Trading Business Service: Balances, Transaction Summary, Login, Options Trading, and Place Order.

- Several applications: Reporting Service, Authentication Service, Trade Service, Order Engine, Reporting Engine, and Authentication Engine. In terms of USM, these applications are named Transaction Contexts of the Application type. Internally, CA APM typically names these applications *frontends*.
- Several *backend* systems. CA APM also detects several database instances. All these backend systems are represented in USM by Software Components of various types (database, sockets, and so on).

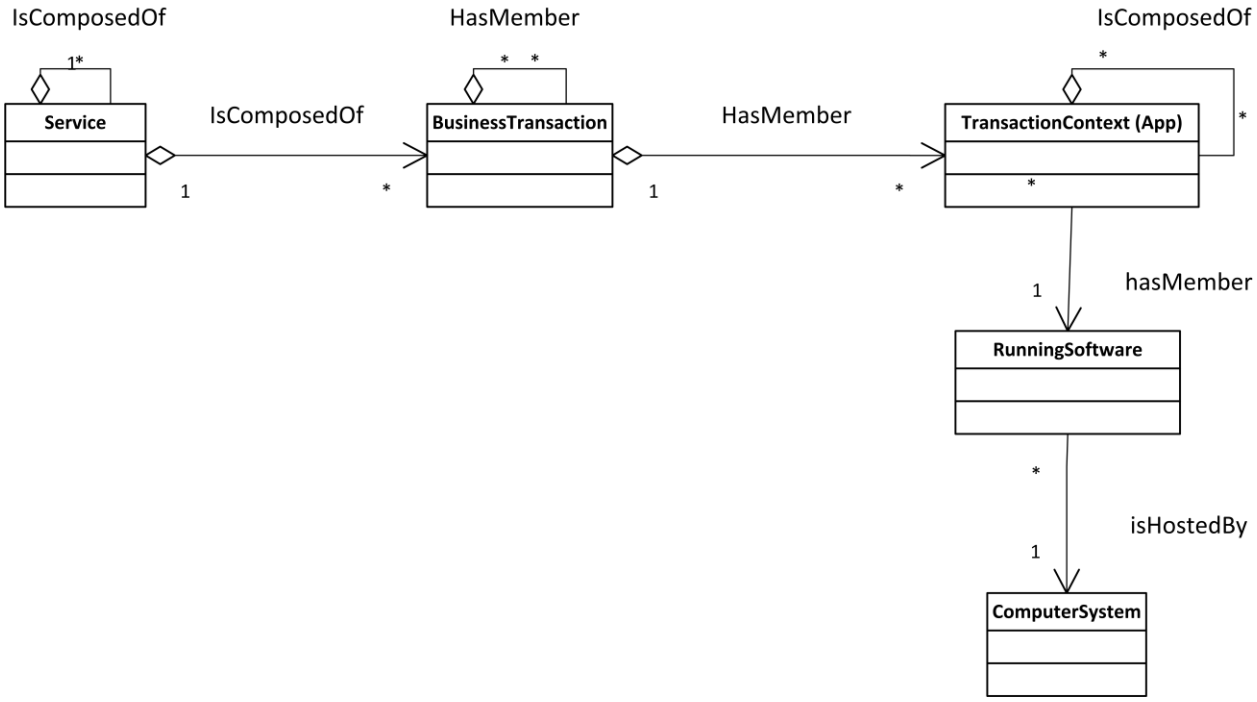
ServiceImportMode App

The App mode designates the frontend where the alert was generated. The TransactionContext is filtered so only data of the type Application is accepted. The service model uses the App mode to obtain:

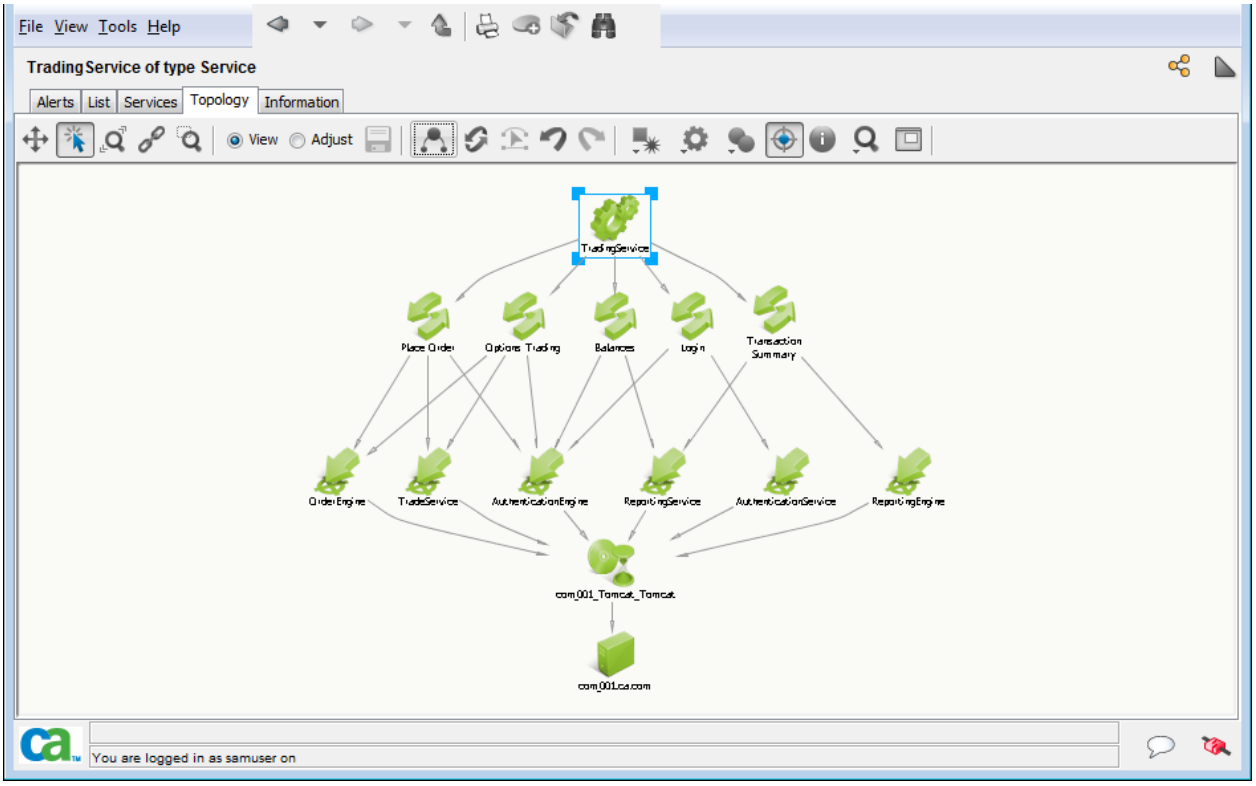
- Metrics-based CA Introscope® alerts which are associated with a service under Running Software CI.
- CA CEM incidents and Triage Map alerts. These incidents and alerts are associated with the Business Transaction and Transaction Context CIs.

This service model supports the following hierarchy using the App mode:

- Service *isComposedOf* multiple BusinessTransactions
  - BusinessTransaction *HasMember* TransactionContext (Application) TransactionContext (Application) *HasMember* RunningSoftware
    - RunningSoftware *isHostedBy* ComputerSystem



The following diagram shows the result of a Service Import when you configure the connector for App mode for the Trade Service application Triage Map example (see page 63):



ServiceImportMode MacOnly

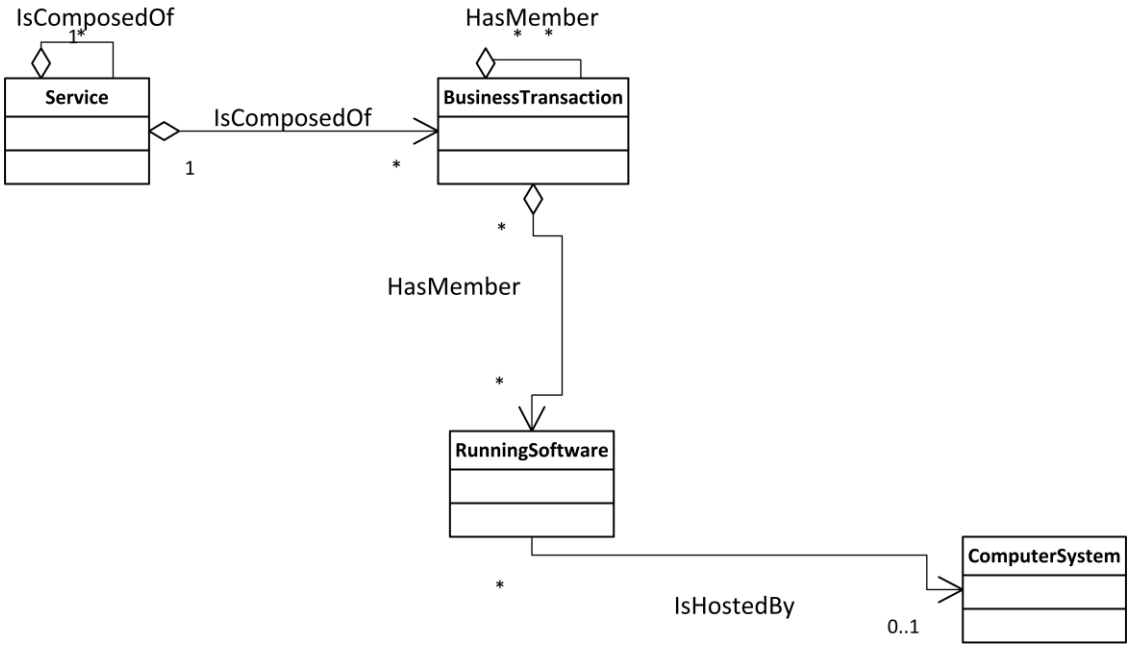
The MacOnly mode specifies that the Transaction Context (that is, frontend application) does not appear. The service model uses the MacOnly mode to obtain:

- Metrics-based CA Introscope® alerts which are associated with a service under Running Software CI.
- CA CEM incidents and Triage Map alerts. These incidents and alerts are associated with the Business Transaction CI.

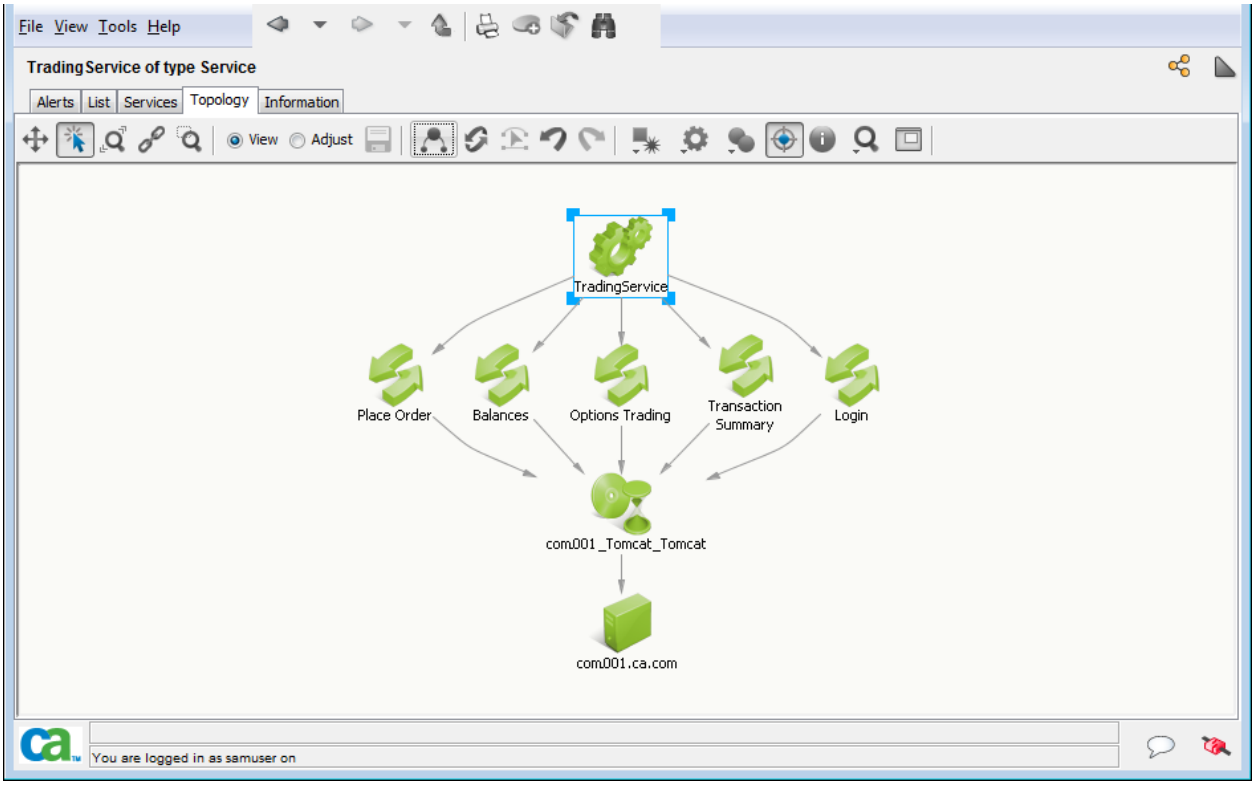
Note: This mode is the default.

This service model supports the following hierarchy using the MacOnly mode:

- Service *isComposedOf* multiple BusinessTransactions
  - BusinessTransaction *HasMember* RunningSoftware
    - RunningSoftware *isHostedBy* ComputerSystem



The following diagram shows the result of a Service Import when you configure the connector for MacOnly mode for the Trade Service application Triage Map example (see page 63).



ServiceImportMode TxTriage

The TxTriage mode displays Software Component CIs which are backends in CA APM of type sockets and databases.

Note: Set the EMGetAllCIs property to Yes to enable this service mode. If you do not set EMGetAllCIs to Yes, the service model appears the same as in MacOnly mode.

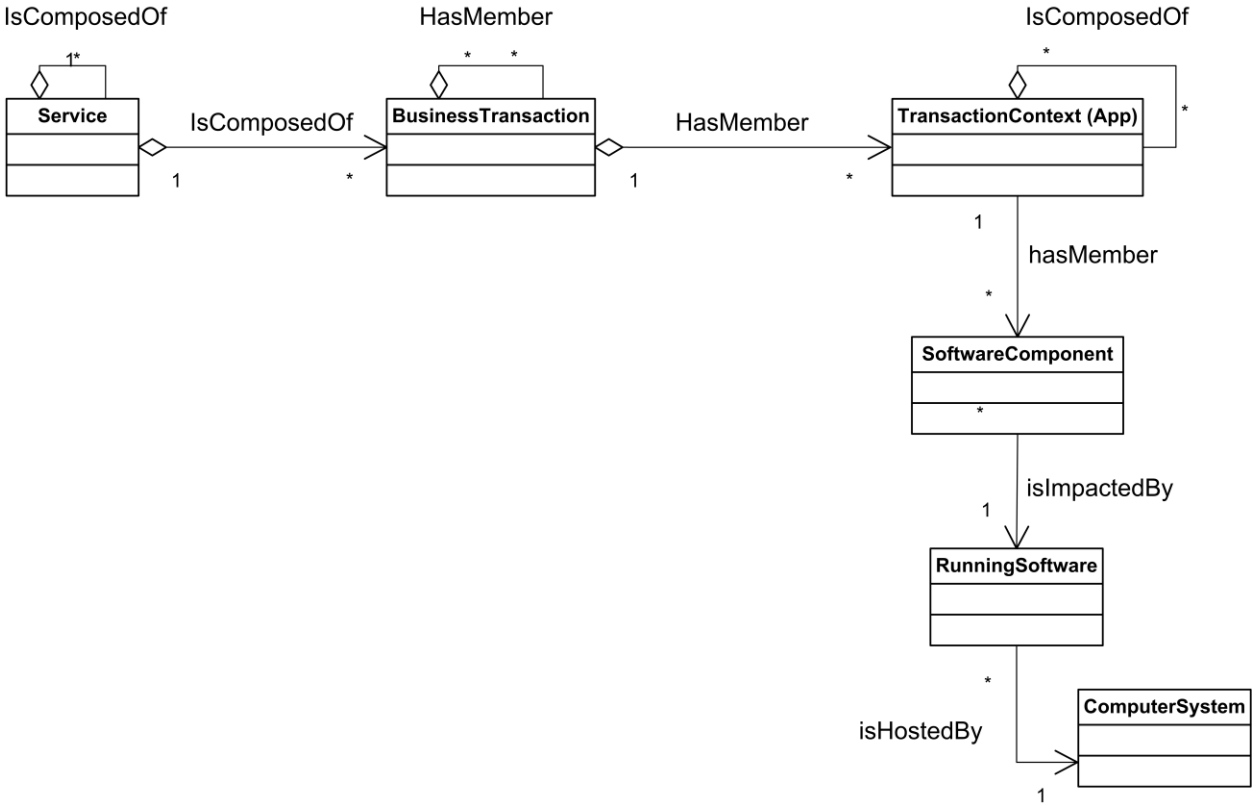
The service model uses the TxTriage mode to:

- Obtain metrics-based CA Introscope® alerts which are associated with a service under Running Software CI.
- Obtain CA CEM incidents and Triage Map alerts. These incidents and alerts are associated with the Business Transaction and Transaction Context CIs.
- Display the relationships between Transaction Context (frontend applications) and their associated Software Components (backends of type sockets and databases).

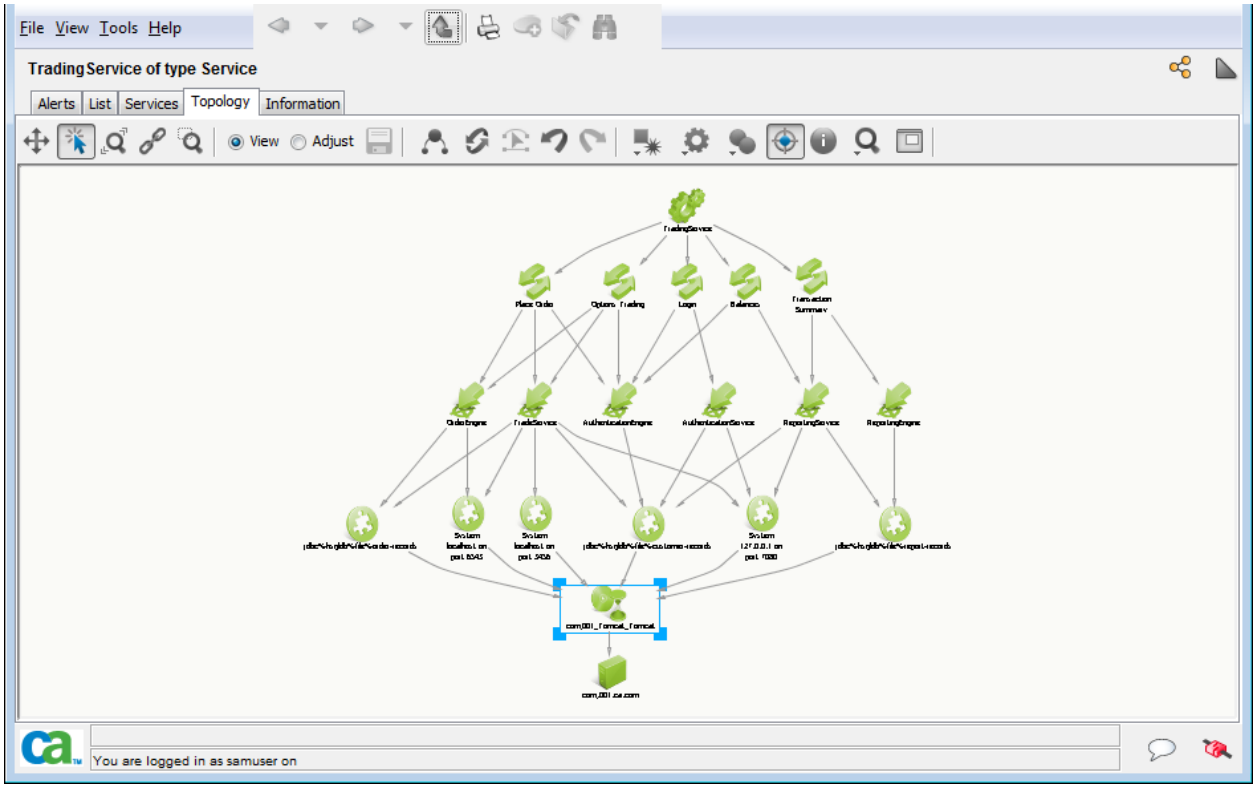
Note: For an integration that connects to a CA APM Enterprise Manager version prior to CA APM 9.6, the mode is the default of MacOnly. The integration uses the MacOnly mode even when the TxTriage import mode is configured on the connector.

This service model supports the following hierarchy using the TxTriage mode:

- Service *isComposedOf* multiple BusinessTransactions
  - BusinessTransaction *HasMember* TransactionContext (Application) TransactionContext (Application) *HasMember* SoftwareComponent SoftwareComponent *isImpactedBy* RunningSoftware
    - RunningSoftware *isHostedBy* ComputerSystem



The following diagram shows the result of a Service Import when you configure the connector for TxTriage mode for the Trade Service application Triage Map example (see page 63):



Appendix A: Troubleshooting

This section contains information for troubleshooting the CA APM Catalyst Connector.

This section contains the following topics:

APM Connector is Offline

If the APM Connector is offline, then perform the following steps:

1. Verify that the "CA SOI Integration Services" is up and running.
2. Verify that the APM connector is listed in the SSA/SOI Portal.
3. Make sure the following properties in <*SOI_HOME*>\resources\Configurations\APM_<*EM_Host*>.xml have been set correctly:

   ```
   EMHost = Host name or IP address where the CA APM Enterprise Manager is installed.

   EMSNMPHostIPAddress=IP address of the Enterprise Manager

   EMSNMPBindAddress=IP address of the APM Catalyst connector
   ```

Important! You must use the IP addresses and not the hostname.

No Introscope Alerts

If no CA Introscope® alert data appears in CA SOI, perform the following steps:

1. Verify that all required patches are installed.
2. Use the “Test Now” capability of the SNMP Alert Action. Verify that the test traps are being received from EM to the CA APM Catalyst Connector by checking the APM_connector.log.

3. Ensure that the following SNMP Alert action properties match the one from the CA APM Catalyst Connector config file (APM_<*EM_Host*>.xml):

   “SNMP Destination > Trap Port” = APM_<EM_Host>.xml > EMSNMPTrapPort

   “SNMP Destination > Community” = APM_<EM_Host>.xml> = EMSNMPCommunity

What to Collect to Escalate an Issue

If the problem persists, contact Support, collect relevant files, and attach the files to the incident.

Follow these steps:

1. Stop CA SAM Integration Services or APM Connector from the Administration tab.
2. Delete the logs from <*SOI_HOME*>\logs and <*SSA_HOME*>\jsw\logs.
3. Enable debug in the C:\Program Files\CA\SSA\resources\Configurations\log4j\APM_log4j.xml file:

   ```
   <logger name="com.ca.wily.apm" additivity="false">
   <level value="TRACE"/>
   <appender-ref ref="APMConnector"/>
   </logger>
   ```

   Note: For the most granular logging information, set the logging level to TRACE.

   TRACE is a more detailed DEBUG version as defined in log4j.
4. Start CA SAM Integration Services.
5. Generate alerts from CA Introscope®.
6. Check for messages in <*SOI_HOME*>\logs\ifw.log similar to the following example (where computer221 is your computer name):
   - 2011-08-13 07:36:30,305 INFO [com.ca.sam.ifw.eventplus.catalog.plugin.IFWWriter:Write] jms.JMSPublisher - Publishing Alert: [CA:00001:computer221:AL:computer221_WebLogic Agent_GC Heap:Bytes In Use]. Shows that alerts are being published.
7. Collect the following files:
   - Zipped content of the <*SOI_HOME*>\logs
   - Zipped content of the <*SOI_HOME*>\jsw\logs
   - Zipped content of the <*SOI_HOME*>\Resources\configurations\
   - Zipped content of the <*EM_HOME*>\logs
   - zipped content of the <*AGENT_HOME*>\logs

8. A screenshot of the SNMP alert definition from the Workstation.
9. A screenshot of the APM_agent table content of the APM database.
10. A general overview of the implementation indicating where SOI, APM Connector, CA Introscope® Enterprise Manager, and agents are present.

Connector 2.x Deployed Against an APM EM Desktop Build

If you deploy a connector to work against a desktop build of the CA APM Enterprise Manager, you must manually edit the APMVersion property in the *APM_<EM_Host>.xml* file.

Example:

```
<property name="APMVersion" value="PostAPM906"/>
```

Note: You must add the APMVersion property only when using a desktop version of the Enterprise Manager. Refer to the Troubleshooting section for more information.

APMVersion Property

To enable the Connector to know what kind of alert information will be received, the Connector will read the APMVersion parameter from the Connector's configuration settings file and run in a ServiceImportMode that fits the version of CA Introscope® which is being asked for alert information. You must add the APMVersion property manually to the *APM_<EM_Host>.xml* file.

Default value: APM95

Possible values:PreApm906, APM906, PostAPM906, APM9071, APM91, APM95, APM96

PreAPM906

If you are accessing a pre-9.0.6 version of CA APM, you will not be able to utilize the complete Service Model or Alerting for CA CEM. You can get legacy alerts for CA Introscope® which will not be associated with any service, but will be associated with newly created Running Software CIs.

APM906

If you are accessing a 9.0.6.0 or 9.0.6.1 version of CA APM, you will get Business Service and Business Transaction data in the Service Model, and you can get CA CEM incidents associated with a Business Transaction. You can get legacy alerts for CA Introscope® which will not be associated with any service, but will be associated with newly created Running Software CIs.

PostAPM906

If you are accessing APM version 9.0.6.2 and above, you can get the complete Service Model, depending on the ServiceImportMode setting. You can get alerts on RunningSoftware CIs, as well as CEM incidents associated with Business Transactions (BTs).

APM9071

This fixes the issue when business transactions with identical transaction names across business services, are monitored by multiple agents, and result in incorrect service model topologies being displayed in SSA/SOI.

APM91

Use this value for APM 9.1 or later versions. This adds triage map support.

APM95

Use this value for APM 9.5 or later versions. This adds support for delete functionality which provides information about the deleted CIs on APM to Catalyst, so that APM related USM objects are in sync.

APM96

Use this value for APM 9.6 or later versions. This adds support for TxTriage mode of Service Import.

Identify the APM Catalyst Connector Version

You can identify the version of CA APM Catalyst Connector you are using.

Note: The versions suggested in the following locations do not provide accurate information about the version of CA APM Catalyst Connector you are using:

- SSA/SOI Web UI, Administration tab, APM Connector status pane
- SOI/SSA Console, Connection Status console

Follow these steps:

1. Browse to the <*SOI_HOME*>\logs.
2. Open the APM_Connector.log file and look for the APM connector version.

   Logging uses the RollingFileAppender in log4j. The log shows the APM connector version depending on how long the APM connector has been running and the size of the APM connector log. If the log does not show the version, restart the CA APM Catalyst Connector or the SSA Integration service and try again.

Index