CA Service Operations Insight

Troubleshooting Guide

r3.2

ca technologies

This Documentation, which includes embedded help systems and electronically distributed materials, (hereinafter referred to as the “Documentation”) is for your informational purposes only and is subject to change or withdrawal by CA at any time. This Documentation is proprietary information of CA and may not be copied, transferred, reproduced, disclosed, modified or duplicated, in whole or in part, without the prior written consent of CA.

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

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

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

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

The manufacturer of this Documentation is CA.

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

CA Technologies Product References

This document references the following CA Technologies products:

- CA Application Performance Management
- CA Business Intelligence
- CA Clarity™ Project and Portfolio Manager
- CA CMDB
- CA Configuration Automation (formerly CA Application Configuration Manager)
- CA eHealth® Performance Manager (CA eHealth)
- CA Embedded Entitlements Manager (CA EEM)
- CA Event Integration
- CA Insight™ Database Performance Manager
- CA NSM
- CA Process Automation
- CA Service Desk
- CA Server Automation (formerly CA Spectrum® Automation Manager)
- CA SiteMinder®
- CA Spectrum®
- CA Systems Performance for Infrastructure Managers
- CA SystemEDGE
- CA Virtual Assurance

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: About This Guide 9

Intended Audience 9
Related Publications 9
Local Documentation and Online Bookshelf 11

Chapter 2: Configuring and Using Diagnostic Tools 13

Debug Consoles 13
- Access the Debug Consoles 14
- SA Manager Debug Console 15
- UI Server Debug Console 18

Using Log Files for Diagnosis 20
- Updated Log File Names 26
- Reorganization of the SA Manager Logs 26
- Logging in the CA SOI IFW 27
- Connector-specific Logging 27
- Configure Event Management Logging 28
- View and Manage the Client Log (client.log) 29
- View and Manage the UI Server Connection Log 30
- Control the Rolling Behavior of the Client Log File 31
- Isolate CA Catalyst Logging Information from soimgr.log 32

Manage the Debug Level for Specific Modules 33
Using Services for Diagnosis 35
- Manage Services 37

Using the Status Bar for Diagnosis 38
- Verify the Connection Status of Components 38

Using the Administration Tab for Diagnosis 39
Set Notifications for the OutOfMemory Conditions on the SA Manager 41
CI Flow in CA SOI and Log File Outputs 42
- CI Flow in CA SOI: Connectors 43
- CI Flow in CA SOI: SA Manager 44
- CI Flow in CA SOI: CA Catalyst 45

Alert Flow in CA SOI and Log File Outputs 46
- Alert Flow in CA SOI: Connectors 47
- Alert Flow in CA SOI: Mid-Tier Connector 49
- Alert Flow in CA SOI: SA Manager 50
- Alert Flow in CA SOI: CA Catalyst 51

Configure Failure Email Notifications....52
Loop Detection During Impact Analysis....53
Connector Shutdown Notifications....53
How to Track Alerts and CIs from CA Spectrum to CA SOI Using Debug Logs....54
How to Track Alerts from CA Spectrum to CA SOI Using Debug Logs....55
How to Track CIs from CA Spectrum to CA SOI Using Debug Logs....61
Trace a CI Using USM Web View for Diagnosing Synchronization Errors....66
Use the CA Catalyst Trace UI for Diagnosing Synchronization Errors....67
CA Catalyst Trace UI Processing Flow....68
CA SOI Toolbox Utility....69
Configuration Options....70
Service Related Action Commands....72
Connector and Database Related Action Commands....72
Database Cleanup Commands....73
How to Clean Up Data with the CA SOI Toolbox....74
CA SOI Toolbox Prerequisites....76
Determine Database Sizing....76
Open the Toolbox with a Command Prompt....79
Create a CA SOI Toolbox Configuration File....80
Clean Up History Data....81
Clean Up Imported Connector Data....82
Chapter 3: Troubleshooting 83
Important! Before Troubleshooting a Problem....83
CA Catalyst Troubleshooting....83
Synchronization - Priming Utility Runs for Hours....84
Installation or Initialization Errors....84
ActiveMQ Server Errors....85
Registry Errors....86
Correlation and Persistence Errors....87
Notification Manager Errors....87
Reconciliation Errors....88
Synchronization Errors....88
Connectors Troubleshooting....90
Alert Synchronization Not Working for a Connector....90
CA Spectrum Connector Binding in a Dual NIC Environment....91
CA Spectrum Connector Keeps Reinitializing....92
CA Spectrum Connector Firewall Limitations....92
Change Connector Credentials....92
Connector Data Not Imported....93
Connector Not Online....94

Connector Unable to Connect to the SSL-Enabled Domain Manager....94
No Connector Data in the Operations Console....96
Anti-virus Programs Affecting the Connector Performance....96
How Do I Troubleshoot Connector Connection Problems?....97
How Do I Troubleshoot the Event Connector?....98
How Do I Troubleshoot the Connector Policy?....98
How to Troubleshoot Connector Shutdown Behavior....99
Sample Connector Changes Are Not Reflected in CA SOI....103
Unable to View CA Catalyst r3.2 Connectors in CA SOI r3.x....104
Verify the Universal Connector Web Service....104
Verify the Universal Connector Files....105
Dashboard Troubleshooting....105
Administration Tab or Dashboard Links Not Working with Firefox....105
Administration Tab Values Not Saving....106
Alerts Not Created....106
CIs Not Created....107
Failure Notification Emails Not Sending....107
Google Earth Does Not Display New or Updated Locations on the Map....107
Event Management Troubleshooting....108
Event Management Connection Problems....108
Event Search Returns no Results or Unexpected Results....108
Expected Alerts Not Appearing on Operations Console After Processing....109
Event Policies Not Producing Expected Actions....109
How Do I Control the Event Management Data Flow to the Operations Console?....110
Searches Taking Too Long....111
Error Messages on an Event Result Error Dialog....111
How to Search Archived Event Store Files?....114
Not Enough Event Groups in Search Results....115
Event Processing Performance Due to Mid-Tier Connector....116
Help Desk Integrations Troubleshooting....116
CA Service Desk Integration Troubleshooting....117
CA Service Desk Ticket Not Created by Escalation Policy Action....117
Cannot Create a BMC Remedy or HP Service Manager Ticket in CA SOI....118
HP Service Manager Integration Troubleshooting....118
Ticket Creation, Closure, or Update is Failing....119
Ticket Status Changed when Connector Shut Down or Removed....119
Integration Framework Troubleshooting....119
Java Heap Space Out Of Memory Error....120
Mobile Dashboard Troubleshooting....120
Service Names do not Appear on the Mobile Dashboard....120
Operations Console Troubleshooting....121
Access - Proxy Server Prompt Opens When Accessing the Operations Console....121

Access - Unable to Start the Operations Console 122
Alerts - How Do I Find an Alert? 122
CIs - Domain Manager Administrative CI States not Reflected in CA SOI 123
CIs - Duplicates Appear on the Operations Console 123
CIs - How Do I Find a CI? 123
CIs - Missing from CA SOI 124
CIs - Property Values are Incorrect 124
Escalation Actions - CA Process Automation Forms Not Available 125
Escalation Actions - Email Actions Not Sending 125
Escalation Actions - Tickets Not Created 126
Escalation Actions - Resolve Escalation Action Failures 126
Service Discovery - Default Significance does not Match CI Significance 128
Service Models - Resolve Looping Problems 128
SLA Recurrence Not Triggering 129
SA Manager and UI Server Troubleshooting 129
Disk Full 129
Error with Browser-Based UIs 130
Resolve an SA Store Database Connection Failure 131
Resolve a Third-Party Server Connection Failure 131
SA Manager Crashing on Startup or Dumping Memory and Performing Slowly 132
[WrapperStartStopAppMain] Warning 132
SOI Toolbox Troubleshooting 133
Toolbox Fails to Run 133
USM Web View Troubleshooting 133
USM Web View Does Not Display All CIs 134
USM Web View Search Returns Incorrect Results 134

Chapter 1: About This Guide

This *Troubleshooting Guide* contains information to diagnose and resolve end-user problems in CA SOI. The guide also provides information and procedures to use the diagnostic tools available in CA SOI.

This section contains the following topics:

Intended Audience (see page 9)
Related Publications (see page 9)
Local Documentation and Online Bookshelf (see page 11)

Intended Audience

This guide is intended for administrators with an advanced understanding of CA SOI and its components. Most operations that are described in this guide require administrator-level permissions in the product.

Related Publications

The following publications, provided on the installation media and the CA SOI online bookshelf, provide complete information about CA SOI:

Administration Guide

Provides information about administering and maintaining the product after installation.

Connector Guide

Provides general information about connectors, the CA Catalyst infrastructure, and writing custom connectors.

Event and Alert Management Best Practices Guide

Provides concepts, procedures, and best practices for managing the event and alert stream that CA SOI receives from connectors.

Implementation Guide

Provides information about installing and implementing the product.

Online Help

Provides information about performing tasks in CA SOI user interfaces.

Readme

Provides information about known issues and information that is discovered after the guides were finalized. A CA SOI release may not have a Readme.

Release Notes

Provides information about operating system support, system requirements, database requirements, web browser support, and international support.

Service Modeling Best Practices Guide

Provides procedures and best practices for modeling services including the following methods: service imports, service discovery, and manual service modeling.

User Guide

Provides information for nonadministrative users about using the product, such as responding to alerts and viewing reports.

Web Services Reference Guide

Provides information about the CA SOI web services for interacting with resources such as CIs, services, alerts, relationships, and escalation policy.

Local Documentation and Online Bookshelf

CA SOI provides access to the documentation locally and online.

Local Documentation

The local documentation is installed in the SOI_HOME\Documentation folder and includes the PDFs for all guides. The online help is also installed with CA SOI and accessed through the Dashboard (PC and Mobile) and USM Web View. The local documentation is updated with specific releases only.

Online Bookshelf

The online bookshelf is on support.ca.com and provides the most current documentation set, which can be updated between releases. The online bookshelf also provides the documentation for the latest supported versions of CA Business Intelligence, CA EEM, and CA Process Automation. For a list of Bookshelf updates, click the Update History link on the Bookshelf.

CA SOI provides access to the online bookshelf in the following locations:

- The Dashboard provides a Bookshelf link.
- The Operations Console provides a menu link under Help, Bookshelf.

Note: If you are unable to access the online bookshelf, contact your system administrator to provide the documentation set PDFs.

Chapter 2: Configuring and Using Diagnostic Tools

This section provides the different high-level methods that you can use to diagnose CA SOI problems.

This section contains the following topics:

Debug Consoles (see page 13)
Using Log Files for Diagnosis (see page 20)
Manage the Debug Level for Specific Modules (see page 33)
Using Services for Diagnosis (see page 35)
Using the Status Bar for Diagnosis (see page 38)
Using the Administration Tab for Diagnosis (see page 39)
Set Notifications for the OutOfMemory Conditions on the SA Manager (see page 41)
CI Flow in CA SOI and Log File Outputs (see page 42)
Alert Flow in CA SOI and Log File Outputs (see page 46)
Configure Failure Email Notifications (see page 52)
How to Track Alerts and CIs from CA Spectrum to CA SOI Using Debug Logs (see page 54)
Trace a CI Using USM Web View for Diagnosing Synchronization Errors (see page 66)
Use the CA Catalyst Trace UI for Diagnosing Synchronization Errors (see page 67)
CA SOI Toolbox Utility (see page 69)
How to Clean Up Data with the CA SOI Toolbox (see page 74)

Debug Consoles

As an administrator, you use the CA SOI Debug Consoles to test and debug various CA SOI components. Many troubleshooting topics direct you to use these pages to diagnose problems. We recommend that you use these pages only when you are directed by a troubleshooting topic.

Each Debug Console provides procedures for using the page. The troubleshooting topics also provide the specific Debug Console options to select, fields to complete, and so on.

The topics that follow provide an overview of the Debug Console functionality.

Access the Debug Consoles

SA Manager Debug Console

You access the CA SOI Console Debug Console on the SA Manager server using the following URL:

http://manager_host:manager*_port/*sam/debug/

manager_host

Specifies the server where the SA Manager resides that was specified during the CA SOI installation.

manager_port

Specifies the Tomcat port that is used for the SA Manager Server HTTP communication and that was specified during the CA SOI installation.

Default: 7090.

UI Server Debug Console

You access the CA SOI UI Server Debug Console on the UI Server using the following URL:

http://*uiserver_host*:*ui_port/*sam/debug/

uiserver_host

Specifies the server where the UI Server resides that was specified during the CA SOI installation.

ui_port

Specifies the Tomcat port that is used for UI Server HTTP communication and that was specified the during CA SOI installation.

Default: 7070.

SA Manager Debug Console

The following debug pages are available on the SA Manager server:

Note: Click Show Usage on any debug page to view detailed page usage procedures.

Troubleshooting

Triage Tests

Use this page to determine the subsystem availability to help you diagnose subsystem failures. This test is generally your first step in troubleshooting many *major* problems. If any Triage Tests fail, you must resolve those failures before any other problems. For more information, see SA Manager Triage Tests (see page 17).

Debug Controller

Use this page to activate the debug features for various modules and log to the soimgr-debug.log file (see page 20). Troubleshooting topics ask you to turn on the certain logging feature when diagnosing problems. The advanced options let you separate or group the logging into one or more files.

Note: We recommend that you turn on each logging option only as you need the information. Excessive logging can both slow down your system and make the log file difficult to read.

Server Log Scanner

Use this page to search for a string in one or more CA SOI log files (see page 20) that are available on this server. This search is similar to a grep utility. Found search strings are indicated in red in the log file. The search results also include the log file line numbers and character location. The embedded links allow you to inspect the log contents quickly. A summary function provides an outline of possible problems that are found in the log file.

Consolidated Log Scanner

Use this page to search the soimgr-error.log file (see page 20). You can search for connection errors and you can see information from particular sources.

Logs

Log Download

Use this page to package and download log files that you want to archive or for working with CA Support technicians.

Web Server Log

Use this page to view and search the current segment of the soimgr.log file (see page 20). This page is useful if you cannot access a server remotely to view a log file.

Consolidated Error Log

Use this page to display the soimgr-error.log file (see page 20). You can optionally show the log starting from a particular search string.

Debug Pages

Memory Usage

Use this page to view the server's memory for diagnosing performance issues. You can run the Java Garbage Collection mechanism to manage Java memory. You can set the page to refresh automatically at regular intervals. You can also toggle logging memory information to the soimgr.log (see page 20) file.

Thread Info

Use this page to generate a Java Virtual Machine (JVM) thread dump when you are trying to diagnose a problem on the JVM. You can see which threads are most active.

Queue Monitor

Use this page to monitor the sizes of thread pools and their associated job queues.

Database Connectivity

Use this page to validate the SA Store Database connection and test the access time. The test parameters are configurable. You can also generate a report.

Database Tables

Use this page to inspect and report on the SA Store database table sizes for troubleshooting database problems and determining when the database requires maintenance. You can also generate, package, and download a report.

Event Integration KPIs

Use this page to display CA SOI event integration key performance indicators (KPIs).

Service Check

Use this page to scan and validate the SA Manager Server services so you can diagnose a service corruption. You can also view service statistics such as the number of CIs.

Layout Check

Use this page to scan and validate the internal service layout (topology) XML descriptors so you can diagnose layout issues. It is nearly impossible to see these layouts in the database itself.

SA Manager Triage Tests

The SA Manager Triage Tests, help you to diagnose major system problems.

Once you access the SA Manager Debug Console and click Triage Tests, click the Show usage link to view how to run the tests.

The SA Manager Triage Tests page provides the following test results:

Base Test

The Base Test section is an overall sanity test of the platform. The tests verify the mechanisms to run the Triage Tests. Any failure can indicate a major problem. A failure can indicate possible problems with the embedded CA Catalyst module. Restart the SA Manager server. If the Base Test fails again, contact CA Support.

Manager Base

The Manager Base section determines if the basic SA Manager components are working. Manager Base failures can indicate an SA Store Database problem.

Access Manager

The Access Manager section indicates possible problems that are related to CA EEM. Failures indicate a problem related to the CA EEM availability or content.

Manager Services

The Manager Services section indicates possible problems that are related to the alert repository, the escalation policies, and the help desk connection.

Auxiliary

Ignore this section. This is for future auxiliary tests.

UI Server Debug Console

Note: Click Show Usage on any debug page to view detailed page usage procedures.

Troubleshooting

Triage Tests

Use this page to determine the subsystem availability to help you diagnose subsystem failures. This test is generally your first step in troubleshooting many *major* problems. For more information, see UI Server Triage Tests (see page 19).

Debug Controller

Use this page to activate the debug features for various modules and log to the soimgr-debug.log file (see page 20). Troubleshooting topics ask you to turn on the certain logging feature when diagnosing problems. The advanced options let you separate or group the logging into one or more files.

Note: We recommend that you turn on each logging option only as you need the information. Excessive logging can both slow down your system and make the log file difficult to read.

Server Log Scanner

Use this page to search for a string in one or more CA SOI log files (see page 20) that are available on this server. This search is similar to a grep utility. Found search strings are indicated in red in the log file. The search results also include the log file line numbers and character location. The embedded links allow you to inspect the log contents quickly. A summary function provides an outline of possible problems that are found in the log file.

Logs

Log Download

Use this page to package and download log files that you want to archive or for working with CA Support technicians.

Web Server Log

Use this page to view and search the current segment of the soiuis.log file (see page 20). This page is useful if you cannot access a server remotely to view the log file.

Debug Pages

Memory Usage

Use this page to view the server's memory for diagnosing performance issues. You can run the Java Garbage Collection mechanism to manage Java memory. You can set the page to refresh automatically at regular intervals. You can also toggle logging memory information to the soiuis.log file (see page 20).

Thread Info

Use this page to generate a Java Virtual Machine (JVM) thread dump when you are trying to diagnose a problem on the virtual machine. You can see which threads are most active.

Queue Monitor

Use this page to monitor the thread pools and their associated queue sizes.

Database Connectivity

Use this page to validate the SA Store Database connection and test the access time. The test parameters are configurable. You can also generate a report.

Synchronization Tests

Use this page to test the repository synchronization between the UI Server and the SA Manager.

Start Client Debug Console

Use this page to set debugging levels for various CA SOI features such as model security, service modeler tree, and users. You view the debugging output in the Java Console, which you enable separately from the Windows Java Control Panel.

UI Server Triage Tests

The UI Server Triage Tests, help you to diagnose major system problems.

Once you access the SA Manager Debug Console and click Triage Tests, click the Show usage link to view how to run the tests.

The UI Server Triage Tests page provides the following test results:

Base Test

The Base Test section is an overall sanity test of the platform. The tests verify the mechanisms to run the Triage Tests. Any failure indicate a possible major problem. Restart the UI Server. If the Base Test fails again, contact CA Support.

UI Server Base

The UI Server Base section determines if the basic UI Server components are working. A failure indicates possible problems with the type repository or a problem on the SA Manager.

Access Manager

The Access Manager section indicates possible problems that are related to CA EEM. Failures are either related to the CA EEM availability or content.

Domain Services

The Domain Services section tests the ability of the UI Server to connect to the SA Manager. A failure indicates a possible communication problem between the UI Server and the SA Manager.

Auxiliary

You can ignore this section. This is for future auxiliary tests.

Using Log Files for Diagnosis

As an administrator, you can use log files to diagnose problems. This section includes information about various log files that help you troubleshoot CA SOI. You can search the contents of many log files on the SA Manager Debug Console (see page 15) and the UI Server Debug Console (see page 18).

BiConfig.log

Helps you troubleshoot reporting import errors. This file is available at SOI_HOME\Reports.

catalyst.log

Contains information specific to CA Catalyst transactions. This file is available at SOI_HOME\tomcat\logs.

CA-SSA-LogicInstallDebug.log

Tracks the Logic Server installation. Use this file to troubleshoot Logic Server installation problems. This CA Catalyst log file is available at SOI_HOME\log.

CA-SSA-RegistryInstallDebug.log

Tracks the Registry installation. Use this file to troubleshoot Registry installation problems. This CA Catalyst log file is available at SOI_HOME\log.

CA-SSA_RestUIInstallDebug.log

Tracks the USM Web View installation. This file is available at SOI_HOME\log.

CA_Event_Integration_InstallLog.log

Includes Event connector-related installation information such as installation errors related to the file copies and configuration settings. This Event connector log file is located in the root of the installation directory.

ci-invalid.log

Tracks the details about CIs with duplicate sheets. If you do not see a CI in CA SOI, check this file to see if it is a duplicate sheet and the limit for duplicates has been reached for that reconciled sheet. This file is available at SOI_HOME\tomcat\logs.

client.log

Contains an entry for every UI Server that is connected to the SA Manager and records for each user connection. This file is available at SOI_HOME\tomcat\webapps\sam\console\logs. The Client Log page lets you view the contents of the client.log file. You can also use this page to clear the log and remove old entries.

connmgr.log

Traces data that the SA Manager receives from the connectors. The Connector Manager option on the Administration UI debug page controls this log file. This file is available at SOI_HOME\tomcat\logs.

Note: For more information about the improved SA Manager logs reorganization, see the Reorganization of the SA Manager Logs (see page 26) section.

Domain_Install_*releasenumber*.log

Tracks the CA SOI Domain connector installation. This file is created when you click Done after the CA SOI Domain connector installation finishes. This file is available at SOI_HOME\log.

eitransform.log

Contains information about all policy operations (such as parse, normalize, and format) included in your connector policy. You can find the eitransform.log file at SOI_HOME\log after it is enabled (see page 98).

EventMgmt.log

Includes Event Management information. By default, the log level in the file is set to INFO. This file is available at SOI_HOME\log. Use this file to troubleshoot the Event Management-related errors.

Example: Search on the Universal connector unexpectedly returning no events

This example considers an example search on the Universal connector that unexpectedly returned no events. After configuring a DEBUG log level and running the search again, the following search information is logged in the file:

```
INFO   | jvm 1    | 2011/04/05 10:02:51 | 10:02:51,063  INFO SDOFactory:208 -
com.ca.eventmanager.operations.EventManagerImpl.getEvents: Incoming
Map:key=(Connectors) Value=(CA:09997_server01.ca.com@server01.ca.com)
INFO   | jvm 1    | 2011/04/05 10:02:51 | 10:02:51,063  INFO SDOFactory:208 -
com.ca.eventmanager.operations.EventManagerImpl.getEvents: Incoming
Map:key=(MdrProduct) Value=(CA:09997)
INFO   | jvm 1    | 2011/04/05 10:02:51 | 10:02:51,063  INFO SDOFactory:208 -
com.ca.eventmanager.operations.EventManagerImpl.getEvents: Incoming
Map:key=(scope.query.operator) Value=(OR)
```

```
INFO   | jvm 1    | 2011/04/05 10:02:51 | 10:02:51,063  INFO SDOFactory:208 -
com.ca.eventmanager.operations.EventManagerImpl.getEvents: Incoming
Map:key=(scope.query.timelast) Value=(1)
...
INFO   | jvm 1    | 2011/04/05 10:02:51 | 10:02:51,141 DEBUG XQueryHelper:95 -
com.ca.eventmanager.common.XQueryHelper.setTimeLast: timelast=1
qp.timestart=1302008571  qp.timeend=1302012171
INFO   | jvm 1    | 2011/04/05 10:02:51 | 10:02:51,141 DEBUG XQueryHelper:96 -
com.ca.eventmanager.common.XQueryHelper.setTimeLast: qp.timestart.epoch=Apr 5,
2011 9:02:51 AM  qp.timeend.epoch=Apr 5, 2011 10:02:51 AM
INFO   | jvm 1    | 2011/04/05 10:02:51 | total reccount=0
INFO   | jvm 1    | 2011/04/05 10:02:51 | timescoped files: 0
INFO   | jvm 1    | 2011/04/05 10:02:51 | recordscoped files:
INFO   | jvm 1    | 2011/04/05 10:02:51 | final-query: let $a :=
doc('file:/C:/Program%20Files/CA/SOI/resources/Core/EventStore/temp/results27
890.xml0.xml')/results/normal return if (count($a)>0) then (<group
id='0'>{$a}</group>) else ()
INFO   | jvm 1    | 2011/04/05 10:02:51 | resultsfile: C:\Program
Files\CA\SOI\resources\Core\EventStore\temp\results27890.xml
...
INFO   | jvm 1    | 2011/04/05 10:02:52 | 10:02:52,219  INFO SDOFactory:208 -
com.ca.eventmanager.operations.EventManagerImpl.getEvents: Returning from
DataSource:SSA key=(Result) Value=(<results scopedeventcount='0'
returnedeventcount='0' warning='' error='pattern_not_matched'> set log4j level
to TRACE to log entire result set.)
```

Note: For more information about this example, see the *Administration Guide*.

EventManagement_wrapper.log

Contains status details of the CA SAM Event Management service. This file is available at SOI_HOME\jsw\logs.

generic_client.log

Tracks web services transactions that the Universal connector client makes. This file is available at SOI_HOME\log. The SOI_HOME\lib\generic\log4j.xml file controls this log. The default level is ERROR. Set to DEBUG to trace transactions.

ifw.log

Contains connector processing details. This file is available at SOI_HOME\log. By default, the debug level is set to ERROR. The IFW appender in SOI_HOME\resources\log4j.xml controls the log levels. If you set a log level, you do not need to restart the system. In general, the log levels produce this type of information:

- INFO: Represents the messages pertaining to the IFW and connector health
- DEBUG: Represents the data being published and received; also creates log\debugData files
- TRACE: Represents the specific methods being called (code trace)

- ERROR: Represents the error messages that are returned from connectors or IFW
- FATAL: Represents the non-recoverable errors

When the IFW appender is set to DEBUG, the SOI_HOME\log\debugData folder contains the following types of files:

- *HEARTBEAT_PUB.txt: Includes status details of IFW or connectors
- *RAW.txt: Includes CI, Alert, and Relationship details per connector prior to normalization through EI
- *PUB.txt: Includes CI, Alert, Relationship details per connector after EI normalization

indexer-catalyst.log

Includes detailed logging for the CA SAM Store Indexer service. This file is available at SOI_HOME\jsw\logs. The SOI_HOME\indexer\log4j.properties file controls this log.

install.log

Includes Event connector-related pre- or post-installation errors such as database creation failure and connector registration problems. This log file is available at EI_HOME\logs.

IntegrationServices_Install_*releasenumber*.log

Includes IFW installation errors. Use this file to troubleshoot the IFW installation issues. This file is available at SOI_HOME\log.

MidTier_Install_*releasenumber*

Tracks installation errors that are related to the Mid-tier connector installation. This file is available at SOI_HOME\log.

registry.log

Tracks the Registry activity. Use this file to troubleshoot the Registry problems. This CA Catalyst log file is available at SOI_HOME\tomcat\logs.

Sample_Install_*releasenumber*.log

Tracks installation errors that are related to the Sample connector. This file is created when you click Done after the Sample connector installation finishes. The file is available at SOI_HOME\log.

SAM-IntegrationServices_wrapper.log

Contains status and general information regarding the Integration Services process and the connectors. This file is available at SOI_HOME\jsw\logs. This log file acts as a primary runtime log file and includes basic runtime informational messages. Anything that is written to *stdout* is captured in this file. You can check the file to determine the following information:

- Why the Integration Services service is not running.
- Why a connector is not running or is in a particular state.

Example: AMQ connection failure

This example shows the ActiveMQ server connection failure information that is logged in the file:

```
INFO   | jvm 1    | 2009/03/20 09:24:57 | AMQPublisher@server1.ca.com: Trying to
establish connection with AMQ.
```

```
INFO   | jvm 1    | 2009/03/20 09:24:58 | AMQPublisher@server1.ca.com: AMQ
Connection failed. User name or password is invalid.
```

SAM_Tomcat_wrapper.log

Includes status information and general processing details from the CA SAM Application Server service. This file is available at SOI_HOME\jsw\logs.

SAM-UI_Server_wrapper.log

Includes status information and general processing details from the CA SAM User Interface Server service. This file is available at SOI_HOME\jsw\logs.

SAM-StoreIndexer_wrapper.log

Includes status information and general processing details from the CA SAM Store Indexer service. This file is available at SOI_HOME\\jsw\logs.

soimgr.log (and soiuis.log)

Tracks CA SOI and CA Catalyst activity. This file also contains all lifecycle (or heartbeat) messages information.

The file soimgr.log at SOI_HOME\tomcat\logs contains SA Manager-specific information. The file soiuis.log that is available at SOI_HOME\SamUI\logs contains UI Server-specific information.

Note: For more information about the SA Manager logs reorganization, see the Reorganization of the SA Manager Logs (see page 26) section.

soimgr-debug.log (and soiuis-debug.log)

Tracks all debug messages. The soimgr-debug.log file that is available at SOI_HOME\tomcat\logs contains SA Manager-specific information. The file soiuis-debug.log at SOI_HOME\SamUI\logs contains UI Server-specific information.

Note: For more information about the SA Manager logs reorganization, see the Reorganization of the SA Manager Logs (see page 26) section.

soimgr-error.log

Includes a consolidated error log that contains errors from several product components. This file is available at SOI_HOME\tomcat\logs. When you encounter a problem with the product, reference this log file first. The file is accessible from the Operations Console Connection Status dialog and the Connector Configuration page of the Administration UI.

SOI_Install_*releasenumber*.log

Includes CA SOI installation error information. This file is available at SOI_HOME\log.

ssa.log

Includes information about whether USM schema validation failures have occurred. This file is available at SOI_HOME\log.

ssa-mobile.log

Tracks the Mobile Dashboard information. This file is available at SOI_HOME\SAMUI\logs.

ssaweb.log

Includes information that is associated with CA Catalyst USM Web View. This file is available at SOI_HOME\SamUI\logs.

service-discovery.log

Tracks the Service Discovery processing. This file is available at SOI_HOME\log. The *SD* appender in the SOI_HOME\resources\log4j.xml file controls this log.

ServiceDiscovery_InstallLog.log

Tracks the installation of Service Discovery. This file is available at SOI_HOME\log.

trace.log

Includes the Reconciler activity. This CA Catalyst log file is available at SOI_HOME\tomcat\logs.

ucf.log

Tracks the UCF Broker activity. Use this file to troubleshoot synchronization problems that are not occurring in the Logic Server. This CA Catalyst log file is available at SOI_HOME\log.

UCF-Broker_wrapper.log

Includes information about general UCF Broker status and processing. This file is available at SOI_HOME\jsw\logs.

Updated Log File Names

In releases before CA SOI r3.1, the SA Manager Server and UI Server log files had the same names: sam.log, samdebug.log, and samerror.log. In CA SOI r3.1, the log files were renamed to differentiate these logs and were also updated to include "SOI" as the naming prefix.

The log files have the following names:

SA Manager Server Log Files

Old Log File Name	New Log File Name (r3.1 and later)
sam.log	soimgr.log
samdebug.log	soimgr-debug.log
samerror.log	soimgr-error.log

UI Server Log Files

Old Log File Name	New Log File Name (r3.1 and later)
sam.log	soiuis.log
samdebug.log	soiuis-debug.log

Reorganization of the SA Manager Logs

In CA SOI r3.0 SP3, CA SOI improved the organization of the SA Manager logs. The SA Manager logs are now organized into multiple log files instead of the single sam.log file, which was the case in the releases prior to CA SOI r3.0 SP3. Log messages are logically grouped into specific log files depending on the type of log information, which helps you use these files more efficiently. For example, if you are searching for a specific debug message, you can directly go to the soimgr-debug.log file (samdebug.log in CA SOI r3.0 SP3). This log file includes all debug messages. Segregating the log information in this manner helps you quickly identify the related log file and locate the problem message, reducing the time that is taken to fix the issue.

The SA Manager logs are reorganized into three separate log files as follows:

Note: You can find these files at SOI_HOME\tomcat\logs.

- All *lifecycle* (or *heartbeat*) messages are logged in the soimgr.log (sam.log in CA SOI r3.0 SP3) file.
- All debug messages are logged in the soimgr-debug.log (samdebug.log in CA SOI r3.0 SP3) file.

- All messages from the Connector Manager component are logged in the connmgr.log file.

Note: For more information about how to set the debug level for a specific module, see Manage the Debug Level for Specific Modules (see page 33).

Logging in the CA SOI IFW

The connector framework uses the log4j.xml file for logging the related information. The log4j.xml configuration file is available at SOI_HOME\resources. The logging is enabled by default in this log file at the INFO level. Multiple log4j appenders are defined for ActiveMQ, IFW, and so on.

To enable more verbose logging, set a specific logger to DEBUG or TRACE. Additionally, if you want to increase all logging for the framework, set *Root IFW Logger* to DEBUG or TRACE instead of INFO:

```
<!-- ROOT IFW LOGGER -->
<logger name="com.ca.sam.ifw" additivity="false">
    <level value="INFO" />
<appender-ref ref="IFW" />
</logger>
```

Connector-specific Logging

This section provides information about connector-specific logging:

- Connectors can provide their own log4j appenders.
- Log4j configuration of connectors is stored in separate files; for example, <*DomainManager*>_log4j.xml.
- Log4j configuration files of connectors are located under *SOI_HOME*\resources\Configurations\log4j.
- Configuration files contain a connector-specific log4j appender and logger.

Configure Event Management Logging

The Event Management information is logged to the following file:

SOI_HOME\log\EventMgmt.log

By default, the log level in the file is INFO. You can change this level to pinpoint errors if your event searches or policies are not performing as expected.

Follow these steps:

1. Open the following file:

   SOI_HOME\resources\eventManager-log4j.xml

2. Set the priority value to DEBUG as follows, and save and close the file:

   ```
   <root>
   <priority value="DEBUG">
   </priority>
   <appender-ref ref="stdout" />
   </root>
   ```

   The EventMgmt.log file now produces more detailed debug messages.

3. Restart the CA SAM Event Management service.

   The logging change is applied.

Consider an example search on the Universal connector that unexpectedly returned no events. After configuring a DEBUG log level and running the search again, you can see the search details:

```
INFO | jvm 1 | 2011/04/05 10:02:51 | 10:02:51,063 INFO SDOFactory:208 -
com.ca.eventmanager.operations.EventManagerImpl.getEvents: Incoming
Map:key=(Connectors) Value=(CA:09997_server01.ca.com@server01.ca.com)
INFO | jvm 1 | 2011/04/05 10:02:51 | 10:02:51,063 INFO SDOFactory:208 -
com.ca.eventmanager.operations.EventManagerImpl.getEvents: Incoming
Map:key=(MdrProduct) Value=(CA:09997)
INFO | jvm 1 | 2011/04/05 10:02:51 | 10:02:51,063 INFO SDOFactory:208 -
com.ca.eventmanager.operations.EventManagerImpl.getEvents: Incoming
Map:key=(scope.query.operator) Value=(OR)
INFO | jvm 1 | 2011/04/05 10:02:51 | 10:02:51,063 INFO SDOFactory:208 -
com.ca.eventmanager.operations.EventManagerImpl.getEvents: Incoming
Map:key=(scope.query.timelast) Value=(1)
...
INFO | jvm 1 | 2011/04/05 10:02:51 | 10:02:51,141 DEBUG XQueryHelper:95 -
com.ca.eventmanager.common.XQueryHelper.setTimeLast: timelast=1
qp.timestart=1302008571 qp.timeend=1302012171
INFO | jvm 1 | 2011/04/05 10:02:51 | 10:02:51,141 DEBUG XQueryHelper:96 -
com.ca.eventmanager.common.XQueryHelper.setTimeLast: qp.timestart.epoch=Apr 5,
2011 9:02:51 AM qp.timeend.epoch=Apr 5, 2011 10:02:51 AM
```

```
INFO | jvm 1 | 2011/04/05 10:02:51 | total reccount=0
INFO | jvm 1 | 2011/04/05 10:02:51 | timescoped files: 0
INFO | jvm 1 | 2011/04/05 10:02:51 | recordscoped files:
INFO | jvm 1 | 2011/04/05 10:02:51 | final-query: let $a :=
doc('file:/C:/Program%20Files/CA/SOI/resources/Core/EventStore/temp/results27
890.xml0.xml')/results/normal return if (count($a)>0) then (<group
id='0'>{$a}</group>) else ()
INFO | jvm 1 | 2011/04/05 10:02:51 | resultsfile: C:\Program
Files\CA\SOI\resources\Core\EventStore\temp\results27890.xml
...
INFO | jvm 1 | 2011/04/05 10:02:52 | 10:02:52,219 INFO SDOFactory:208 -
com.ca.eventmanager.operations.EventManagerImpl.getEvents: Returning from
DataSource:SSA key=(Result) Value=(<results scopedeventcount='0'
returnedeventcount='0' warning='' error='pattern_not_matched'> set log4j level
to TRACE to log entire result set.)
```

The initial lines define the Universal connector MdrProduct value (CA:00097), the server name (server01.ca.com), and a defined scope to search on events for the last hour. The DEBUG message writes the start and end time of the search (qp.timestart.epoch=Apr 5, 2011 9:02:51 AM qp.timeend.epoch=Apr 5, 2011 10:02:51 AM), which is helpful for determining the files that were searched. Finally, the following message shows that no events were found in the scoped time:

```
INFO | jvm 1 | 2011/04/05 10:02:51 | timescoped files: 0
```

Using this information, you can change the scoped time period and rerun the search.

View and Manage the Client Log (client.log)

The CA SOI installation program installs a client.log file on the SA Manager. By default, it is located at SOI_HOME\tomcat\webapps\sam\console\logs.

The client.log file contains an entry for every user who logs on to the Operations Console. The Client Log page allows you to view the contents of client.log file. You can also use this page to clear the log and remove old entries.

Follow these steps:

1. Launch the Dashboard.
2. Click the Administration tab.
3. Click the plus sign (+) next to the CA Service Operations Insight UI Server Configuration option.
4. Click the plus sign (+) next to the server you want to configure.

   The configuration options appear.
5. Click Client Log.

6. (Optional) Enter a number in the Purge entries older than # days field, and then click Go.

   The log entries older than the specified number of days are removed from the log.

7. (Optional) Click Clear Log.

View and Manage the UI Server Connection Log

The CA SOI provides a client.log file on the SA Manager. By default, it is at SOI_HOME\tomcat\webapps\sam\console\logs.

The client.log file contains an entry for every UI Server that is connected to the SA Manager and records for each user connection. The Client Log page allows you to view the contents of the client.log file. You can also use this page to clear the log and remove old entries.

Follow these steps:

1. Click the Administration tab.

   The administration options appear in the left pane.

2. Click the plus sign (+) next to CA Service Operations Insight Manager Configuration.
3. Click the plus sign (+) next to the server you want to configure.
4. Click UI Server Connection Log.
5. (Optional) Enter a number in the 'Purge entries older than # days' field, and click Go.

   The log entries older than the specified number of days disappear from the log.

6. (Optional) Click Clear Log.

Note: You can perform this procedure on the SA Manager only. The UI Server has a similar feature where you can view and manage the users that are connected to the Operations Console.

Control the Rolling Behavior of the Client Log File

The client.log file contains an entry for every user who logs in to the Operations Console. The Client Log page on the Dashboard Administration tab allows you to view the contents of client.log file. You can also use this page to clear the log and remove old entries. For more information, see the *Administration Guide*.

The CA SOI installation installs a client.log file on the UI Server and SA Manager Server. The file is typically at the following locations:

SOI_HOME\SamUI\webapps\sam\console\logs

SOI_HOME\tomcat\webapps\sam\console\logs

Previously, a server (typically the UI Server) would throw a heap dump if the client.log file grew too large to fit into memory. You then had to purge the log entries manually.

CA SOI now provides a log-rolling behavior so that the file does not grow too large. You can optionally control the rolling behavior with three parameters.

Follow these steps:

1. Depending on which client.log file you are modifying, stop either the CA SAM User Interface Server service or the CA SAM Application Server service.
2. Locate and open the web.xml file, which is typically at the following location:

   SOI_HOME\SAMUI\webapps\sam\WEB-INF
3. Add one or more of the following parameters to the web.xml file:

   MaxLogs

   Specifies the number of log file extents that are maintained in a sequence.

   param-name: com.aprisma.spectrum.app.web.util.MaxLogs

   Default param-value: 10

   MaxSize

   Specifies the maximum log file extent size.

   param-name: com.aprisma.spectrum.app.web.util.MaxSize

   Default param-value: 2,000,000 (bytes)

   Note: The UI Server uses an in-memory DOM representation of the current log that takes up to ten times the file size. Therefore, keep the size of each log extent low. The average size of the entry is about 400 bytes. Therefore, the default of 2 Mb is sufficient for approximately 5000 log on and off entries.

FlushFreq

Specifies the number of log entries that are written between log file size checks.

param-name: com.aprisma.spectrum.app.web.util.FlushFreq

Default param-value: 10

The following sample shows the parameter tags for setting the MaxLogs parameter to a maximum of five extents.

```
<context-param>
  <param-name>com.aprisma.spectrum.app.web.util.MaxLogs</param-name>
  <param-value>5</param-value>
  <description>
      This parameter determines max number of client.log extents.
  </description>
</context-param>
```

4. Save the file and restart the CA SAM User Interface Server service or the CA SAM Application Server service.

Isolate CA Catalyst Logging Information from soimgr.log

You can isolate CA Catalyst-related logging information from soimgr.log in the SOI_HOME\tomcat\lib\log4j.xml file. You add appropriate entries to the log4j.xml file. These entries configure the product to log CA Catalyst-specific information to a separate catalyst.log file. This file would include information from the Persistence Service, Reconciler, Synchronizer, and Notification Manager components.

Follow these steps:

1. Locate and open the SOI_HOME\tomcat\lib\log4j.xml file in a text editor.
2. Add a section to the file similar to the following:

```
<appender name="CAT" class="org.apache.log4j.RollingFileAppender">
    <param name="File" value="&logDir;/catalyst.log"/>
    <param name="Append" value="true"/>
    <param name="MaxFileSize" value="20MB"/>
    <param name="MaxBackupIndex" value="10"/>
    <layout class="org.apache.log4j.PatternLayout">
    <param name="ConversionPattern" value="&filePattern;"/>
    </layout>
</appender>
```

3. Add a logger to the appender with the appropriate log level as follows:

   ```
   <logger name="com.ca.ssa.sor" additivity="false">
       <level value="INFO" />
       <appender-ref ref="CAT" />
   </logger>
   ```

4. Save the changes and close the file.

Manage the Debug Level for Specific Modules

As an administrator, you can use the Debug Controller page to activate, adjust, and manage the debug features of individual CA SOI server modules. You can perform the following tasks on this page:

- Enable (ON) or disable (OFF) the debug state of the module.
- Specify the appropriate granularity (OFF, MIN, MOD, and MAX) for the debug level.
- Specify whether to repeat the debug output of any selected module into a separate log file specific to that module. The separate (*Sep*) option on the page provides this functionality. You can also specify whether to repeat the debug output of all selected modules into the same file. The group (*Grp*) option provides this functionality. You can specify these settings by using the advanced options. Also, consider the following points when using the separate and group options:
  - Separate (Sep) and group (Grp) options are not mutually exclusive.
  - You can activate any number of separate and group options simultaneously.
  - The *Repeater* log output is emitted only if debug for the module is turned on.
  - If the debug level of the module is turned off, the repeater log output is also turned off.

Note: The debug Console is designed to be used only with help from CA Technical Support.

Follow these steps:

1. Click Start, Programs, CA, Service Operations Insight, CA Service Operations Insight User Interface.
2. Enter the appropriate user credentials.

   The Administration UI opens.

3. Click the Administration tab.

   The administration options appear in the left pane.

4. Click the plus sign (+) next to the CA Service Operations Insight Manager Configuration option.

   The available servers appear.

5. Click the name of the required server.

   The page that opens contains the Debugging And Logs button.

6. Click Debugging And Logs and then click the Debug Controller link.

   The Debug Controller page opens.

7. Set the debug level for the specific module as follows:

   Note: You can use the Info icon tooltip (Info column) to view detailed information about the function that a specific module performs.

   - Select ON or OFF in the Desired State column to set the debug state for the module.
   - Select OFF, MIN, MOD, or MAX in the Desired Level column to set the desired debug level granularity.
   - Click the Apply button to save the settings.

     The Current State and Current Debug Level columns start showing the updated state.

   Note: If the entry in the Module Handle column is truncated, the entry tooltip shows the complete debug handle string (used in the web.xml setup) for the module.

8. Click the Advanced Options button if you want to specify the repeater options: separate (Sep) and group (Grp).

   The Debug Controller page is updated with the Repeater Logs column appearing next to the Module Handle column.

9. Select the appropriate repeater option for the module as follows:

   Sep

   Allows the logging subsystem to repeat the debug output of *any* selected module into a separate log file that is dedicated to that module. The tooltip of the separate option (Sep) shows the name of the associated log file. This name is derived from the abbreviated name of the module. For example, if the Sep option is checked for the *Action Service* module, the debug output of the module is duplicated and logged into the *dbg-rpt-actionservice.log* file.

Grp

Allows the logging subsystem to repeat the debug output of *all* selected modules into the same file. The name of the log file that is associated with the group option (Grp) is fixed as *dbg-rpt-customlog.log*. For example, if the Grp option is checked for the *Action Service* and *Action Retry Config* modules, their debug output is duplicated and combined into the *dbg-rpt-customlog.log* file.

10. Click Apply.

    The settings are saved.

Using Services for Diagnosis

As an administrator, you use the following component services that control various operations in CA SOI:

CA SAM Application Server

Controls the operation of the SA Manager. This service is installed on any system that contains the SA Manager component. Some of the examples where you are required to restart this service are as follows:

- You configure the email server to send CA SOI notifications if a *mailhost* DNS alias for the email server does not exist.
- You configure the Mobile Dashboard connection information, USM Web View connection settings, and global settings.
- You configure the eventManagerClientConfig.xml file to decide how you want to control the Event Management data flow to the Operations Console.
- You reconfigure the Persistence Store connectivity.
- You change the administrator password.
- You experience installation errors or have problems initializing CA Catalyst components.

CA SAM Event Management

Controls communication with the Event Store on connector systems for Event Management. This service is installed on any system that contains the SA Manager or a connector. Depending on the status of the service (running or stopped), data sources on the system appear in green (running) or red (stopped). Some of the examples where you are required to restart this service are as follows:

- You configure the Event Management logging.
- You configure the event search settings.

CA SAM Integration Services

Controls the operation of the IFW, which handles the communication between the connectors and the SA Manager. This service is installed on any system that contains a connector or the ActiveMQ Server, which is a component of the SA Manager. Some of the examples where you are required to restart this service are as follows:

- You configure the IFW configuration file.
- You enable a connector that was previously disabled.
- You configure the Event Store parameters.
- You manually deploy a custom connector.
- You change the global alert filter setting.
- You change the global DNS lookup setting.
- You experience installation errors or have problems initializing CA Catalyst components.

CA SAM Store Indexer

Controls the indexing of USM data from the Persistence Store for use by the USM Web View. This service is installed on any system that contains the UI Server. Some of the examples where you are required to restart this service are as follows:

- You change the Persistence Store connectivity while configuring the Registry.
- You change the Solr connectivity as part of the Registry configuration.
- You configure the Registry for the standalone SA Manager installation.
- You experience installation errors or have problems initializing CA Catalyst components.

Note: For specific information about the Persistence Store, see the *Administration Guide*.

CA SAM User Interface Server

Controls the operation of the UI Server, including all user interfaces. This service is installed on any system that contains the UI Server component. Some of the examples where you are required to restart this service are as follows:

- You add custom links to the Dashboard.
- You add custom metrics to the Dashboard.
- You configure the level of services that the Dashboard displays.
- You change the metric icons on the Mobile Dashboard.
- You customize the Mobile Dashboard polling intervals.

- You synchronize the UI Server with the report server.
- You experience installation errors or have problems initializing CA Catalyst components.

CA UCF Broker

Controls the UCF broker, which facilitates create, update, and delete operations from connectors to their source domain managers. This service is installed on any system that contains the SA Manager. Some of the examples where you restart this service are as follows:

- You try to enable the maintenance synchronization in the case no domain manager entry appears in the list.
- You experience installation errors or have problems initializing CA Catalyst components.

Manage Services

You can view the status of each installed service and can start or stop it as required. For example, you can verify that the product installed successfully by checking that all installed services are in the running state. If any service is not running, you can manually restart it.

Follow these steps:

1. Select Start, Settings, Control Panel, Administrative Tools, Services.

   The Services dialog opens.

2. Check for the status of the following services on the appropriate servers, depending on where the components were installed:

   - CA SAM Application Server
   - CA SAM Event Management
   - CA SAM Integration Services
   - CA SAM Store Indexer
   - CA SAM User Interface Server
   - CA UCF Broker

3. Right-click the service name, and select Start (or Stop) from the context menu.

   The service is started or stopped as applicable.

Using the Status Bar for Diagnosis

As administrator, you can use the Status bar at the bottom of the Operations Console to view the status information about the current CA SOI connection. The Status bar contains the following icons:

🔌

Opens the Connection Status (see page 38) dialog, which displays the current connection status of all CA SOI components (SA Manager, UI Server, connectors, and so on).

Note: For the User Management Service, even if CA EEM displays without a version number in the Description column, it does not indicate a problem with the product. The service still displays as Online.

💬

Opens the Messages dialog, which displays any new messages from the administrator.

If the SA Manager connection is lost, the Status bar also displays your user name, the login server, and an alert message.

Verify the Connection Status of Components

You can verify that the connection status of each installed component using the Connection Status dialog. The Connection Status dialog also displays a connection log and an Open Consolidated Error Log button. This log button opens the consolidated log file in a web browser. The Connection icon displays a green icon to indicate that all components have a connected status. The icon displays a red icon to indicate that one or more components have lost connection.

Follow these steps:

1. Select Start, Programs, CA, Service Operations Insight, CA Service Operations Insight User Interface.

   An authentication dialog opens.

2. Enter the Administrator user credentials that you specified during the installation, and click OK.

   The CA SOI Dashboard opens.

3. Click Console.

   The Operations Console opens.

4. Click the Connection icon at the bottom right of the Console.

   The Connection Status dialog opens and displays the connection status of each installed component.

5. Review the information.

Note: If you want to view the message, click the Messages icon . The Messages dialog also displays the message date, time, and sender information.

Using the Administration Tab for Diagnosis

As an administrator, use the Administration tab on the Dashboard to maintain connectors and SA Manager settings. The Administration tab also lets you configure single sign-on using CA EEM, email notifications, and other administrative functions. You can also use the Administration tab with other diagnostic methods to diagnose various issues. Some of the issues that you can diagnose using the Administration tab are as follows:

- You are unable to connect to CA Service Desk or create CA Service Desk in CA SOI. In this case, you can verify that the connection settings are correct on the Help Desk Configuration page of the Administration tab. (Administration, CA Service Operations Insight Manager Configuration, *server_name*.)
- You are not getting any data from your connector. In such situations, you can consider the following points:
  - Verify the status of the connector in the Connector Status field (Administration, Connector Configuration, *server_name*, *connector_name*).
  - Review the associated message in the Status Description field (Administration, Connector Configuration, *server_name*, *connector_name*).
  - Open the consolidated error log file from the Connector Configuration page (Administration, Connector Configuration).
  - Verify the status of the IFW in the Current Integration Framework Status field (Administration, Connector Configuration, *server_name*).
- You are experiencing issues communicating with the CA EEM server. To diagnose this issue, you can verify that the correct CA EEM server-related information is available on the EEM Configuration page on the SA Manager and UI Server. You can also click the Test button to verify whether the connection information is correct.
- You are unable to launch the Mobile Dashboard from the Administration UI. To diagnose this issue, you can review the communication settings for the Mobile Dashboard server on the Mobile Dashboard Server Configuration page (Administration, CA Service Operations Insight Manager Configuration, *server_name*).

- You can view details about the SA Manager to help troubleshoot messaging and database connection issues. Access the Administration, CA Service Operations Insight Manager Configuration, *server_name* page to view the information.

  You can access the SA Server Debug Console on the SA Manager server using the Debugging and Logs button on the Manager Configure page (Administration, CA Service Operations Insight Manager Configuration, *server_name*).

- You are unable to use the $[USM Web View URL] runtime token to invoke USM Web View as part of an escalation action. In this case, you can review and test the connection settings for USM Web View on the USM Web View Configuration page (Administration, CA Service Operations Insight Manager Configuration, *server_name*).

- You can access the UI Server Debug Console on the UI server using the Debugging and Logs button on the UI Server page (Administration, CA Service Operations Insight UI Server Configuration, *server_name*).

- You are unable to invoke CA Process Automation processes in an alert escalation action. In this scenario, you can verify the communication settings for the CA Process Automation server on the Process Automation Server Configuration page (Administration, CA Service Operations Insight Manager Configuration, *server_name*).

- You can review the Client Log page (Administration, CA Service Operations UI Server Configuration, *server_name*) to view the contents of the client.log file. This file contains an entry for every UI Server that is connected to the SA Manager and records for each user connection. You can also use this page to clear the log and remove old entries.

- You are unable to generate reports in CA SOI. In this case, you can verify that CA SOI is configured to access the BusinessObjects report server. Also, verify that all the connection settings on the Configure Report Server page (Administration, CA Service Operations UI Server Configuration, *server_name*) are correct.

Note: For more information about how to access the Administration UI and perform various operations, see the *Administration Guide*.

Set Notifications for the OutOfMemory Conditions on the SA Manager

As an administrator, you can enable email notifications for out-of-memory conditions.

Any exceptions (such as OutOfMemory conditions) on the SA Manager can compromise the stability of the SA Manager if they are left unnoticed. To manage such situations, CA SOI provides a detection mechanism that sends notifications whenever any exception stops the JSW wrapper. CA SOI identifies such scenarios and uses the JSW wrapper to send email notifications to the administrator. The email includes detailed information about the failure condition and the reason about why CA SOI was shut down. The administrator can then analyze the scenario, take appropriate measures to fix the issues, and prevent the SA Manager from growing indefinitely and compromising the stability. To set the email notification, update the SOI_HOME\jsw\conf\EmailNotification.conf file.

Follow these steps:

1. Navigate to the SOI_HOME\jsw\conf folder.
2. Locate and open the EmailNotification.conf file in a text editor.
3. Update the parameters available under various sections of the file as appropriate; for example:

   - To enter the sender and recipient email addresses, update the *wrapper.event.default.email.sender* and *wrapper.event.default.email.recipient* parameters under the *# Common Event Email settings.* section. An example is as follows:

     ```
     wrapper.event.default.email.sender=abc@xyz.com
     wrapper.event.default.email.recipient=def@xyz.com
     ```

   - To update the email server, update the *wrapper.event.default.email.smtp.host=<SMTP Server Host>* entry and modify the SMTP server host with the actual email server the client is using. An example is as follows:

     ```
     wrapper.event.default.email.smtp.host=mail.xyz.com
     ```

   - To receive notifications for any option that is mentioned in the # *Enable specific event emails.* section, uncomment the specific option.

   - To customize the body of the email, update the *wrapper.event.jvm_restart.email.body* parameter under the *# Specify custom mail content* section. An example is as follows:

     ```
     wrapper.event.jvm_restart.email.body=The JVM was restarted.\n\nPlease check
     on its status.\n
     ```

   Note: For more information about various parameters, see http://wrapper.tanukisoftware.com/doc/english/props-event.html#properties.

4. Save the changes in the file.

   The settings are applied.

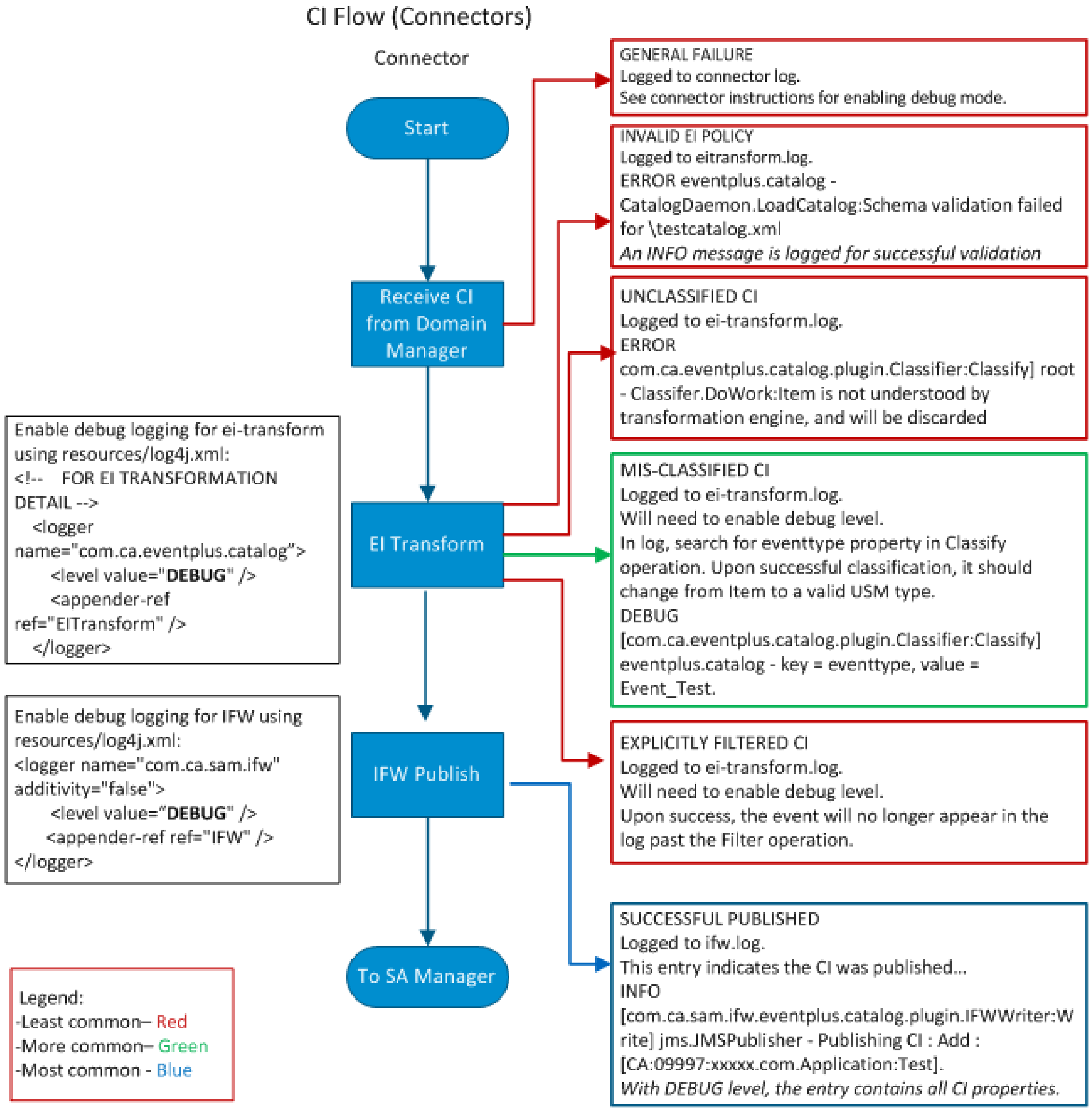
CI Flow in CA SOI and Log File Outputs

As an administrator, use the following graphics to view the flow of CIs through various components. The graphics in each topic also show the outputs that are generated to the log files during the CI flow so that you can trace CIs through the system when necessary.

- CI Flow in CA SOI: Connectors (see page 43)
- CI Flow in CA SOI: SA Manager (see page 44)
- CI Flow in CA SOI: CA Catalyst (see page 45)

CI Flow in CA SOI: Connectors

The following graphic shows the CI flow and related log files in connectors:



GENERAL FAILURE
Logged to connector log.
See connector instructions for enabling debug mode.

INVALID EI POLICY
Logged to eitransform.log.
ERROR eventplus.catalog - CatalogDaemon.LoadCatalog:Schema validation failed for \testcatalog.xml
An INFO message is logged for successful validation

UNCLASSIFIED CI
Logged to ei-transform.log.
ERROR com.ca.eventplus.catalog.plugin.Classifier:Classify] root - Classifer.DoWork:Item is not understood by transformation engine, and will be discarded

MIS-CLASSIFIED CI
Logged to ei-transform.log.
Will need to enable debug level.
In log, search for eventtype property in Classify operation. Upon successful classification, it should change from Item to a valid USM type.
DEBUG [com.ca.eventplus.catalog.plugin.Classifier:Classify] eventplus.catalog - key = eventtype, value = Event_Test.

EXPLICITLY FILTERED CI
Logged to ei-transform.log.
Will need to enable debug level.
Upon success, the event will no longer appear in the log past the Filter operation.

SUCCESSFUL PUBLISHED
Logged to ifw.log.
This entry indicates the CI was published...
INFO [com.ca.sam.ifw.eventplus.catalog.plugin.IFWWriter:Write] jms.JMSPublisher - Publishing CI : Add : [CA:09997:xxxxx.com.Application:Test].
With DEBUG level, the entry contains all CI properties.

Enable debug logging for ei-transform using resources/log4j.xml:

```
<!--    FOR EI TRANSFORMATION
DETAIL -->
   <logger
name="com.ca.eventplus.catalog”>
      <level value="DEBUG" />
      <appender-ref
ref="EITransform" />
   </logger>
```

Enable debug logging for IFW using resources/log4j.xml:

```
<logger name="com.ca.sam.ifw"
additivity="false">
      <level value=“DEBUG" />
     <appender-ref ref="IFW" />
</logger>
```

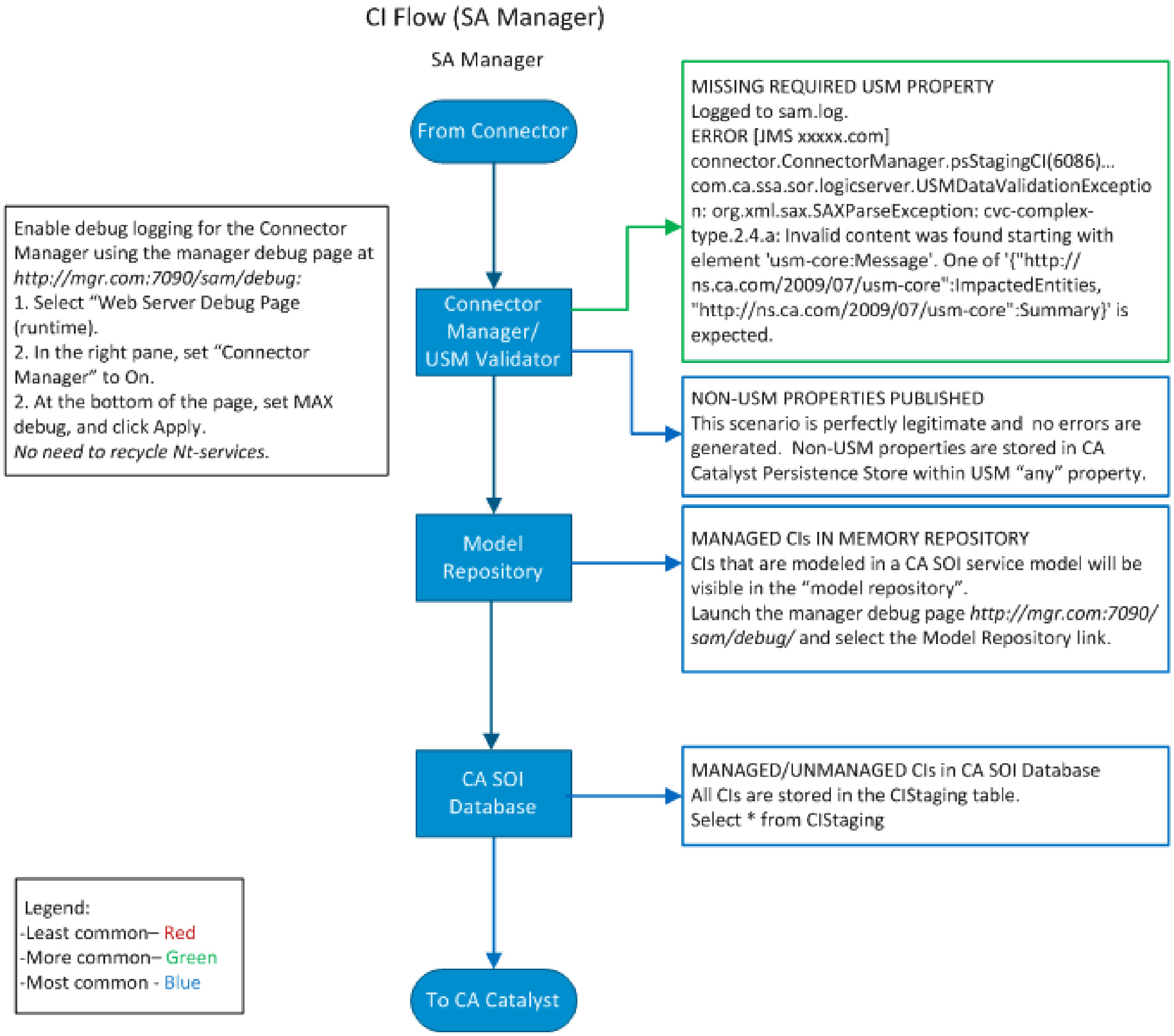
Legend:
-Least common– Red
-More common– Green
-Most common - Blue

The following points explain the information that is covered in the graphic:

- Connector receives CIs from the domain manager.
- CIs are transformed to the USM format.
- Transformed CIs move to the IFW for publishing.
- The IFW publishes transformed CIs to the SA Manager.

CI Flow in CA SOI: SA Manager

The following graphic shows the CI flow and related log files in the SA Manager:



CI Flow (SA Manager)

Enable debug logging for the Connector Manager using the manager debug page at *http://mgr.com:7090/sam/debug:*
1. Select "Web Server Debug Page (runtime).
2. In the right pane, set "Connector Manager" to On.
2. At the bottom of the page, set MAX debug, and click Apply.
No need to recycle Nt-services.

MISSING REQUIRED USM PROPERTY
Logged to sam.log.
ERROR [JMS xxxxx.com] connector.ConnectorManager.psStagingCI(6086)... com.ca.ssa.sor.logicserver.USMDataValidationException: org.xml.sax.SAXParseException: cvc-complex-type.2.4.a: Invalid content was found starting with element 'usm-core:Message'. One of '{"http://ns.ca.com/2009/07/usm-core":ImpactedEntities, "http://ns.ca.com/2009/07/usm-core":Summary}' is expected.

NON-USM PROPERTIES PUBLISHED
This scenario is perfectly legitimate and no errors are generated. Non-USM properties are stored in CA Catalyst Persistence Store within USM "any" property.

MANAGED CIs IN MEMORY REPOSITORY
CIs that are modeled in a CA SOI service model will be visible in the "model repository".
Launch the manager debug page *http://mgr.com:7090/sam/debug/* and select the Model Repository link.

MANAGED/UNMANAGED CIs in CA SOI Database
All CIs are stored in the CIStaging table.
Select * from CIStaging

Legend:
-Least common– Red
-More common– Green
-Most common - Blue

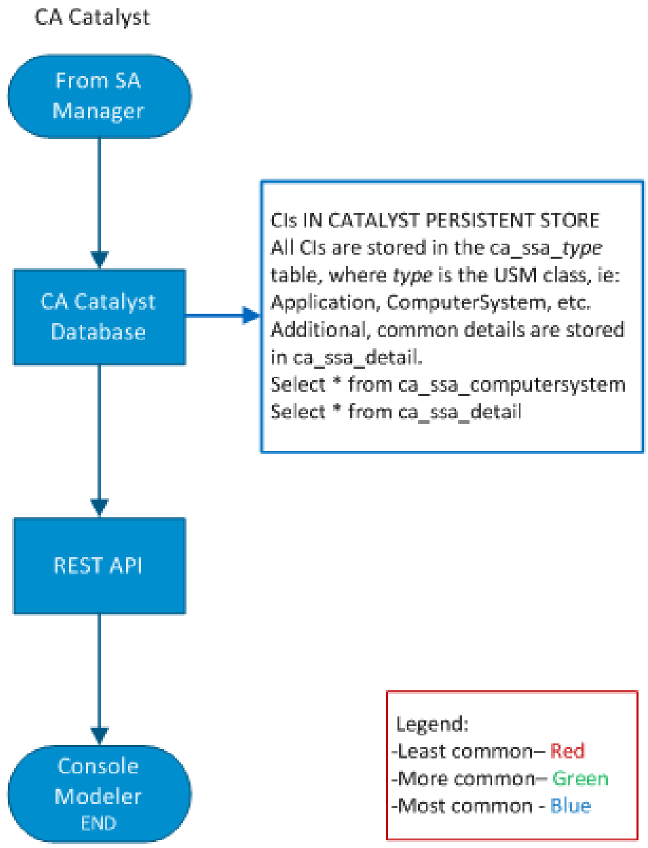
The following points explain the information that is covered in the graphic:

- Connector Manager (or USM Validator) validates the CIs (for example, validates for any missing USM properties) coming from the connector.
- Model Repository maintains and caches the model information. All managed CIs become available in this repository.
- All CIs (managed and unmanaged) are stored in the CA SOI database (SA Store) and become available to CA Catalyst.

CI Flow in CA SOI: CA Catalyst

The following graphic shows the CI flow and related log files in CA Catalyst:

CI Flow (CA Catalyst)


CA Catalyst
From SA Manager
CA Catalyst Database
CIs IN CATALYST PERSISTENT STORE
All CIs are stored in the ca_ssa_*type*
table, where *type* is the USM class, ie:
Application, ComputerSystem, etc.
Additional, common details are stored
in ca_ssa_detail.
Select * from ca_ssa_computersystem
Select * from ca_ssa_detail
REST API
Console Modeler END
Legend:
-Least common– Red
-More common– Green
-Most common - Blue

The following points explain the information that is covered in the graphic:

- All CIs are stored in the CA Catalyst database.
- All stored CIs become available to USM Web View.
- All CIs become available to the Console and Modeler.

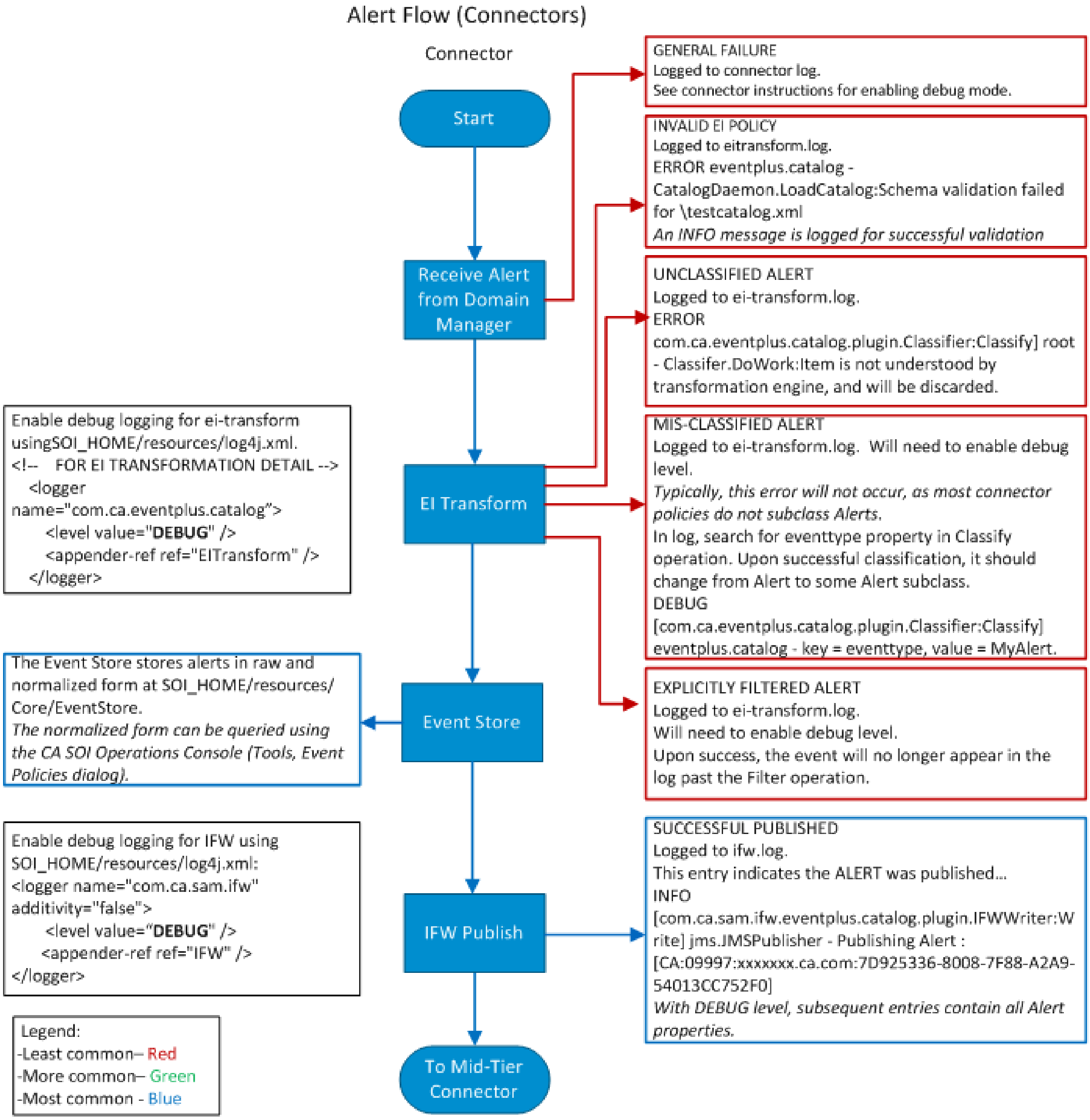
Alert Flow in CA SOI and Log File Outputs

As an administrator, view the following graphics to understand the flow of alerts through various components. The graphics also show the outputs that are generated to the log files during the alert flow so that you can trace alerts through the system when necessary.

- Alert Flow in CA SOI: Connectors (see page 47)
- Alert Flow in CA SOI: Mid-Tier Connector (see page 49)
- Alert Flow in CA SOI: SA Manager (see page 50)
- Alert Flow in CA SOI: CA Catalyst (see page 51)

Alert Flow in CA SOI: Connectors

The following graphic shows the alert flow and related log files in connectors:



Alert Flow (Connectors)

GENERAL FAILURE
Logged to connector log.
See connector instructions for enabling debug mode.

INVALID EI POLICY
Logged to eitransform.log.
ERROR eventplus.catalog - CatalogDaemon.LoadCatalog:Schema validation failed for \testcatalog.xml
An INFO message is logged for successful validation

UNCLASSIFIED ALERT
Logged to ei-transform.log.
ERROR com.ca.eventplus.catalog.plugin.Classifier:Classify] root - Classifer.DoWork:Item is not understood by transformation engine, and will be discarded.

MIS-CLASSIFIED ALERT
Logged to ei-transform.log. Will need to enable debug level.
Typically, this error will not occur, as most connector policies do not subclass Alerts.
In log, search for eventtype property in Classify operation. Upon successful classification, it should change from Alert to some Alert subclass.
DEBUG [com.ca.eventplus.catalog.plugin.Classifier:Classify] eventplus.catalog - key = eventtype, value = MyAlert.

EXPLICITLY FILTERED ALERT
Logged to ei-transform.log.
Will need to enable debug level.
Upon success, the event will no longer appear in the log past the Filter operation.

SUCCESSFUL PUBLISHED
Logged to ifw.log.
This entry indicates the ALERT was published...
INFO [com.ca.sam.ifw.eventplus.catalog.plugin.IFWWriter:Write] jms.JMSPublisher - Publishing Alert : [CA:09997:xxxxxxx.ca.com:7D925336-8008-7F88-A2A9-54013CC752F0]
With DEBUG level, subsequent entries contain all Alert properties.

Enable debug logging for ei-transform usingSOI_HOME/resources/log4j.xml.

```
<!--    FOR EI TRANSFORMATION DETAIL -->
   <logger
name="com.ca.eventplus.catalog">
      <level value="DEBUG" />
      <appender-ref ref="EITransform" />
   </logger>
```

The Event Store stores alerts in raw and normalized form at SOI_HOME/resources/Core/EventStore.
The normalized form can be queried using the CA SOI Operations Console (Tools, Event Policies dialog).

Enable debug logging for IFW using SOI_HOME/resources/log4j.xml:

```
<logger name="com.ca.sam.ifw"
additivity="false">
      <level value="DEBUG" />
     <appender-ref ref="IFW" />
</logger>
```

Legend:
-Least common– Red
-More common– Green
-Most common - Blue

The following points explain the information that is covered in the graphic:

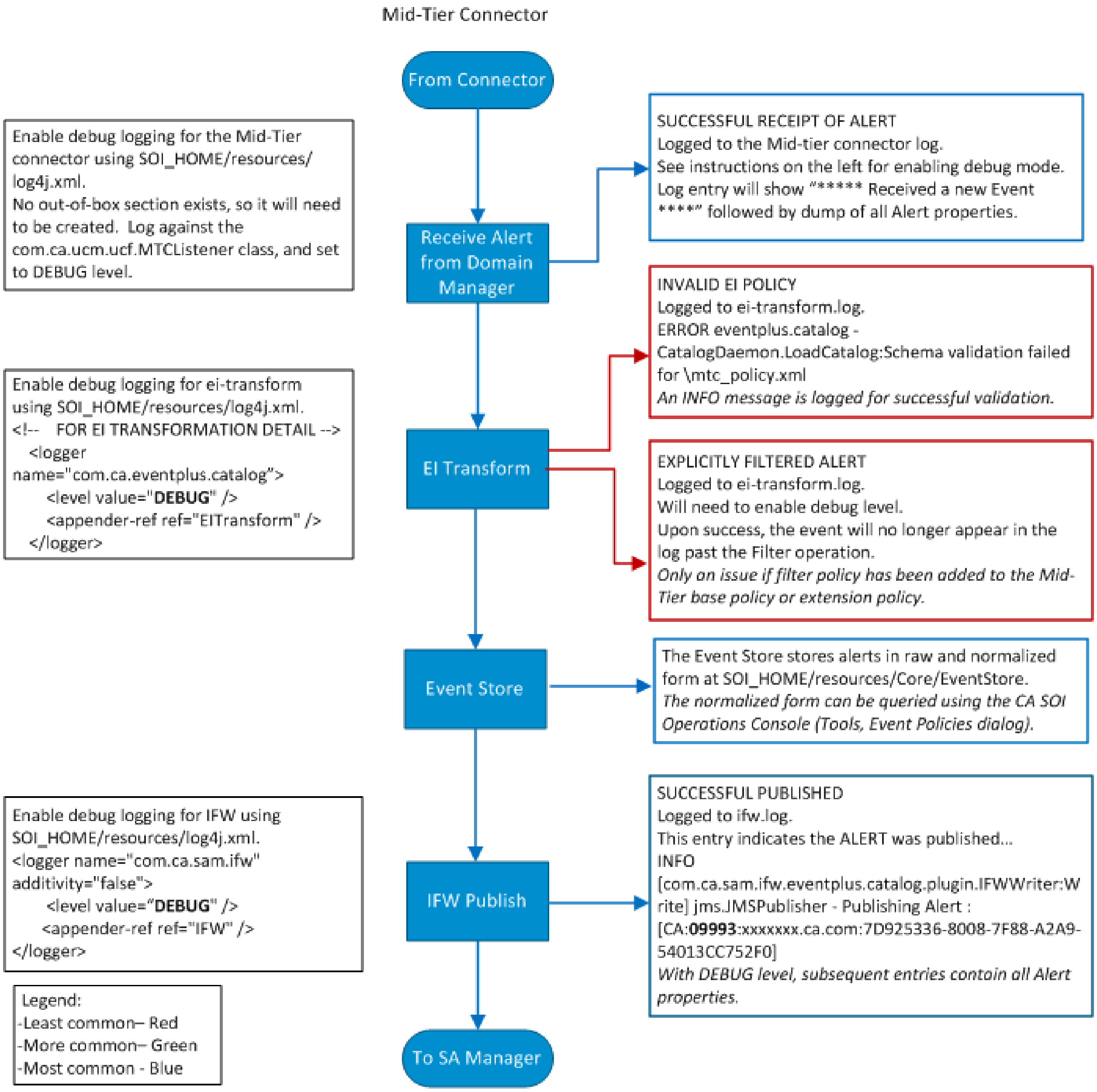
- Connector receives alerts from the domain manager.
- Alerts are transformed to the USM format.
- The Event Store stores all alerts.
- Alerts are passed to the IFW for publishing.
- The IFW publishes transformed alerts to the Mid-Tier connector (if available).

  Note: If the Mid-Tier connector is not present, alerts directly move to the SA Manager.

Alert Flow in CA SOI: Mid-Tier Connector

The following graphic shows the alert flow and related log files in the Mid-Tier connector:

Alert Flow (Mid-Tier Connector)



Enable debug logging for the Mid-Tier connector using SOI_HOME/resources/log4j.xml.
No out-of-box section exists, so it will need to be created. Log against the com.ca.ucm.ucf.MTCListener class, and set to DEBUG level.

Enable debug logging for ei-transform using SOI_HOME/resources/log4j.xml.

```
<!--    FOR EI TRANSFORMATION DETAIL -->
   <logger
name="com.ca.eventplus.catalog">
      <level value="DEBUG" />
      <appender-ref ref="EITransform" />
   </logger>
```

Enable debug logging for IFW using SOI_HOME/resources/log4j.xml.

```
<logger name="com.ca.sam.ifw"
additivity="false">
      <level value="DEBUG" />
      <appender-ref ref="IFW" />
</logger>
```

Legend:
-Least common– Red
-More common– Green
-Most common - Blue

SUCCESSFUL RECEIPT OF ALERT
Logged to the Mid-tier connector log.
See instructions on the left for enabling debug mode.
Log entry will show "***** Received a new Event ****" followed by dump of all Alert properties.

INVALID EI POLICY
Logged to ei-transform.log.
ERROR eventplus.catalog - CatalogDaemon.LoadCatalog:Schema validation failed for \mtc_policy.xml
An INFO message is logged for successful validation.

EXPLICITLY FILTERED ALERT
Logged to ei-transform.log.
Will need to enable debug level.
Upon success, the event will no longer appear in the log past the Filter operation.
Only an issue if filter policy has been added to the Mid-Tier base policy or extension policy.

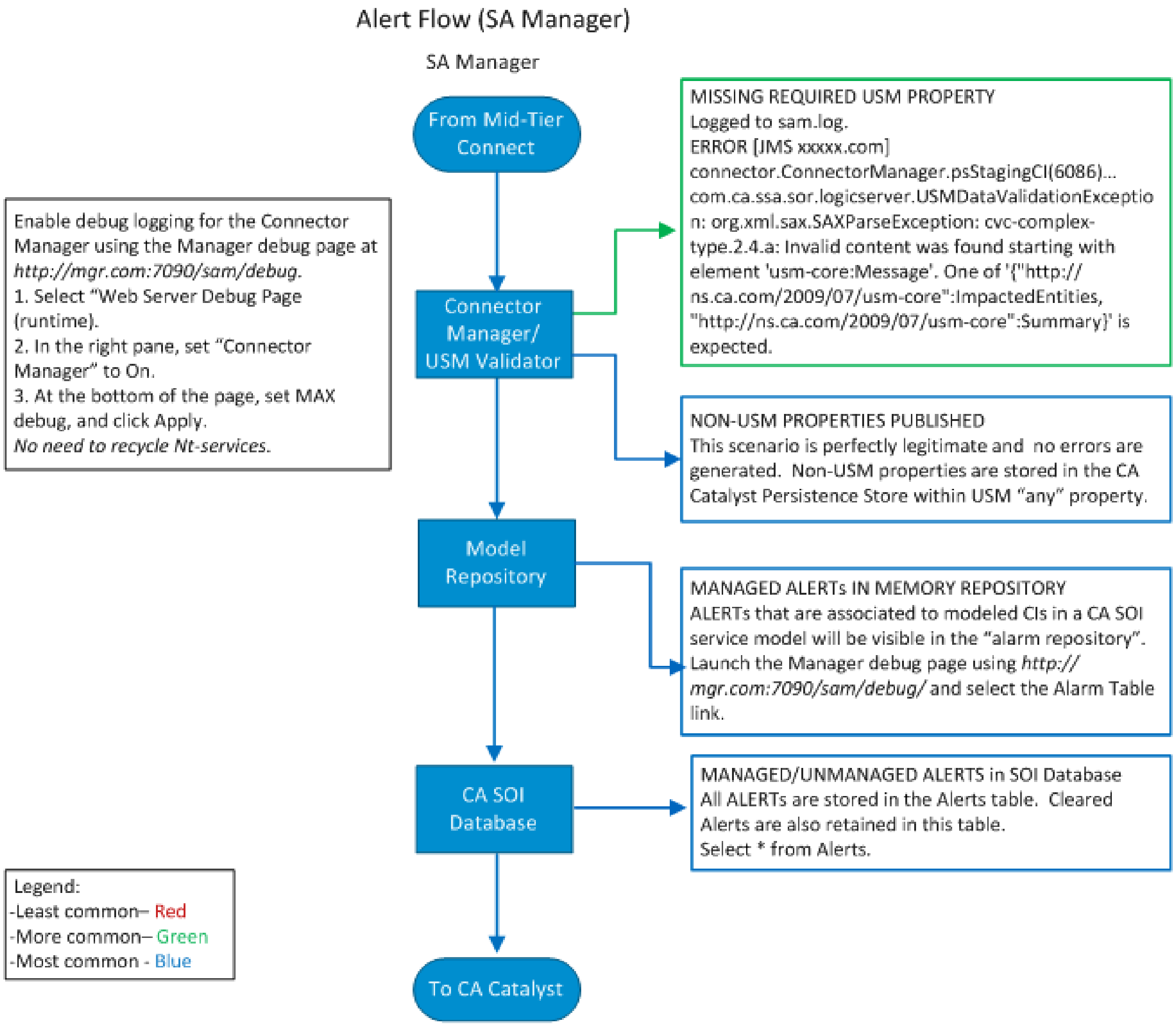
The Event Store stores alerts in raw and normalized form at SOI_HOME/resources/Core/EventStore.
The normalized form can be queried using the CA SOI Operations Console (Tools, Event Policies dialog).

SUCCESSFUL PUBLISHED
Logged to ifw.log.
This entry indicates the ALERT was published...
INFO [com.ca.sam.ifw.eventplus.catalog.plugin.IFWWriter:Write] jms.JMSPublisher - Publishing Alert : [CA:**09993**:xxxxxxx.ca.com:7D925336-8008-7F88-A2A9-54013CC752F0]
With DEBUG level, subsequent entries contain all Alert properties.

The same process is followed as explained in the Alert Flow in CA SOI: Connectors (see page 47) section. However, in this case, the IFW publishes alerts to the SA Manager.

Alert Flow in CA SOI: SA Manager

The following graphic shows the alert flow and related log files in the SA Manager:



Enable debug logging for the Connector Manager using the Manager debug page at *http://mgr.com:7090/sam/debug*.
1. Select "Web Server Debug Page (runtime).
2. In the right pane, set "Connector Manager" to On.
3. At the bottom of the page, set MAX debug, and click Apply.
No need to recycle Nt-services.

MISSING REQUIRED USM PROPERTY
Logged to sam.log.

```
ERROR [JMS xxxxx.com]
connector.ConnectorManager.psStagingCI(6086)...
com.ca.ssa.sor.logicserver.USMDataValidationException: org.xml.sax.SAXParseException: cvc-complex-type.2.4.a: Invalid content was found starting with element 'usm-core:Message'. One of '{"http://ns.ca.com/2009/07/usm-core":ImpactedEntities, "http://ns.ca.com/2009/07/usm-core":Summary}' is expected.
```

NON-USM PROPERTIES PUBLISHED
This scenario is perfectly legitimate and no errors are generated. Non-USM properties are stored in the CA Catalyst Persistence Store within USM "any" property.

MANAGED ALERTs IN MEMORY REPOSITORY
ALERTs that are associated to modeled CIs in a CA SOI service model will be visible in the "alarm repository". Launch the Manager debug page using *http://mgr.com:7090/sam/debug/* and select the Alarm Table link.

MANAGED/UNMANAGED ALERTS in SOI Database
All ALERTs are stored in the Alerts table. Cleared Alerts are also retained in this table.
Select * from Alerts.

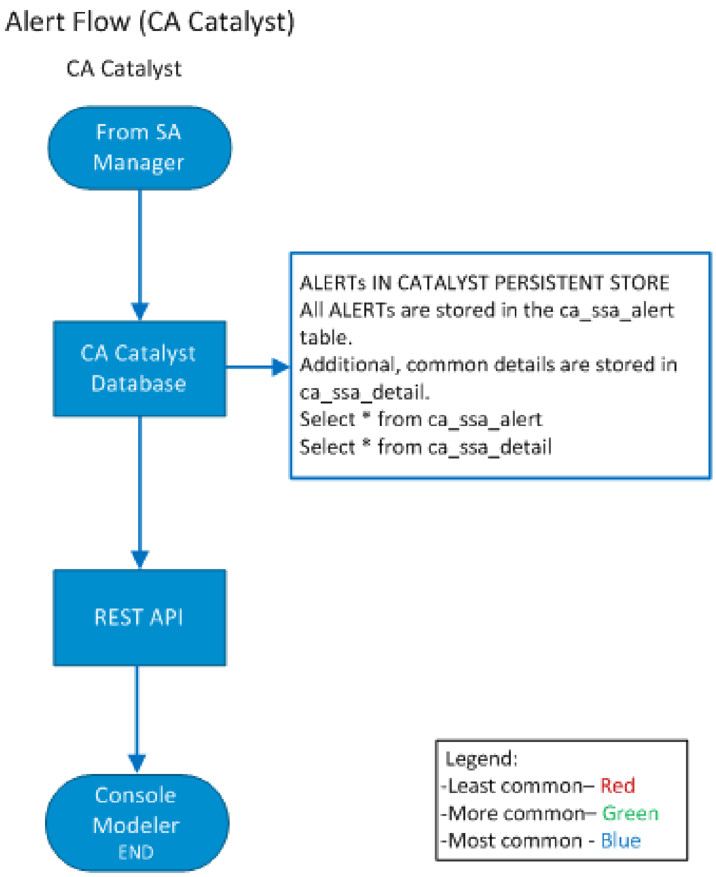
Legend:
-Least common– Red
-More common– Green
-Most common - Blue

The following points explain the information that is covered in the graphic:

- Connector Manager (or USM Validator) validates the alerts (for example, validates for any missing USM properties) coming from the connector (or Mid-Tier connector).
- Model Repository maintains and caches the model information. All managed alerts become available in this repository.
- All alerts (managed and unmanaged) are stored in the CA SOI database (SA Store) and become available to CA Catalyst.

Alert Flow in CA SOI: CA Catalyst

The following graphic shows the alert flow and related log files in CA Catalyst:



ALERTs IN CATALYST PERSISTENT STORE
All ALERTs are stored in the ca_ssa_alert table.
Additional, common details are stored in ca_ssa_detail.
Select * from ca_ssa_alert
Select * from ca_ssa_detail

The following points explain the information that is covered in the graphic:

- All alerts coming from the SA Manager are stored in the CA Catalyst database.
- All stored alerts information becomes available to USM Web View.
- All alerts become available to the Console and Modeler.

Configure Failure Email Notifications

As an administrator, you can configure email notifications to a specified administrator or administrators when certain failures occur. CA SOI also provides logging for the failures:

- The action mechanism fails due to a third-party server connection error. The action mechanism relies on a connection to external servers for the help desk (CA Service Desk), workflows (CA Process Automation), and so on. CA SOI now notifies a specified administrator when the connectivity is lost for more than a specified number of minutes.
- The SA Manager fails due to looping errors. For more information, see Loop Detection during Impact Analysis (see page 53).
- A connection to the SA Store database fails.
- A connector status changes or fails. For more information, see Connector Shutdown Notifications (see page 53).
- After a configured retry duration period, an escalation policy action fails.

The email notifications provide a description of the problem and troubleshooting tips to resolve the problem.

For any failure, CA SOI updates the soimgr.log file (see page 20) with failure information.

Follow these steps:

1. Click the Administration tab.
2. Click the plus sign (+) next to CA SOI Insight Manager Configuration.
3. Click the plus sign (+) next to the server you want to configure.
4. Click Error Notification Configuration.
5. Enter the full email address for the administrator.

   Note: Enter multiple email addresses separated with commas (,).
6. For each notification section, perform the following actions:
   a. Select Yes from the drop-down to turn on email notifications.
   b. Enter the number of minutes until CA SOI sends the email notification.
   c. **Note:** The minimum value is 1 minute.

Loop Detection During Impact Analysis

CA SOI detects loops during an impact analysis. An administrator can configure CA SOI to send an email notification when the SA Manager fails due to looping.

When CA SOI detects a loop in a service or service hierarchy, the SA Manager marks that service as being in TEST mode. This blocks the service state propagation and, in effect, takes the service offline. If the email notification is enabled for the SA Manager events, then CA SOI generates an email. The email contains the name of the service that CA SOI detected the loop in and the SA Manager that CA SOI detected the loop on. To return the service to a production state, edit and then save the service.

When CA SOI detects a loop during an impact analysis, CA SOI appends the following message with the name and internal model handle to the soimgr.log file. CA SOI appends a message each time that CA SOI detects looping.

```
*********************************************************************************
*********************************************************************************
*********************************************************************************
ATTENTION! Loop detected in service 'XYZ' Setting all service properties for
MH(0x10000000003) to TEST
*********************************************************************************
*********************************************************************************
*********************************************************************************
```

Connector Shutdown Notifications

CA SOI provides notifications and detailed logging when a connector shuts down. CA SOI logs and sends an immediate notification to the administrator in the event any connector goes offline for any reason. You can set an interval where CA SOI consolidates all failed connector information into one notification. The improved and faster notification mechanism provides comprehensive information about the connector shutdown behavior, including any appropriate reason for the shutdown. The information in the log messages helps you troubleshoot connectors, audit the connector status in your infrastructure, and take any prompt actions. You can review the related log files to find more information about any anomaly that you encounter in the connector behavior. The easy identification of the problem that is associated with the connector also lets you manage your domain managers more efficiently.

The enhanced connector notification and logging mechanism, therefore, helps you as follows:

- Logs the appropriate reason (for example,connector failure or an IFW shutdown) for the connector shutdown in the log file, SAM-IntegrationServices_wrapper.log. You can review the log file to locate and analyze the message information.

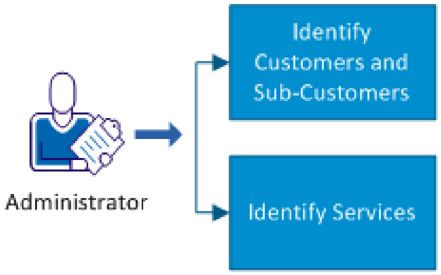
- Includes the shutdown message in the connector status notification as part of the *heartbeat* message. The heartbeat message is logged into the <*ConnectorName*>_HEARTBEAT_PUB.txt. You can review this file to see the message included in the statusDesc property.
- Displays the reason for the connector shutdown in the Administration UI and Console.
- Sends an email notification to the CA SOI administrator about the connector shutdown.

How to Track Alerts and CIs from CA Spectrum to CA SOI Using Debug Logs

As an administrator, you can track the data flow from CA Spectrum to CA SOI to investigate and resolve related issues. This scenario describes how you can enable debug on the CA Spectrum connector. You can then investigate the debug logs to track alerts and CIs as they flow from CA Spectrum to CA SOI.

Use this scenario to guide you through the process:

How to Track Alerts and CIs from CA Spectrum to CA SOI Using Debug Logs



- How to Track Alerts from CA Spectrum to CA SOI Using Debug Logs (see page 55).
- How to Track CIs from CA Spectrum to CA SOI Using Debug Logs (see page 61).

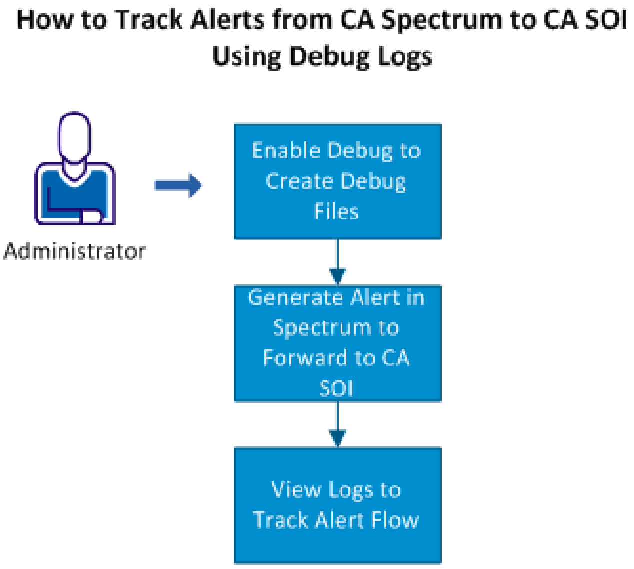
For this example, only one particular device in CA Spectrum has been used against which alerts are created. The alerts are then tracked in the debug files to verify that the alerts are passed from CA Spectrum to the CA Spectrum connector and then to CA Catalyst.

Note: For more information about the command-line interface and Event Configuration interface in CA Spectrum, see the CA Spectrum documentation. For more information about the CA Spectrum connector, see the *CA Spectrum Connector Guide*.

How to Track Alerts from CA Spectrum to CA SOI Using Debug Logs

As a CA SOI administration, you can enable debug on the CA Spectrum connector and can investigate the debug logs to track alerts as they flow from CA Spectrum to CA SOI.

Use this scenario to guide you through the process:


How to Track Alerts from CA Spectrum to CA SOI Using Debug Logs
Administrator
Enable Debug to Create Debug Files
Generate Alert in Spectrum to Forward to CA SOI
View Logs to Track Alert Flow

1. Enable Debug to Create Debug Files (see page 55).
2. Generate an Alert in CA Spectrum to Forward to CA SOI (see page 56).
3. View Logs to Track the Flow of Alerts (see page 57).
   a. View Alert_RAW File (see page 58).
   b. View Alert_PUB File (see page 59).

Enable Debug to Create Debug Files

This procedure provides information about how to enable debug to create the debug files that you can use to track alerts from CA Spectrum to CA SOI.

Follow these steps:

1. Navigate to the SOI_HOME\resources folder on the computer where the CA Spectrum connector is installed.
2. Locate and open the log4j.xml file.

   The file opens in a text editor.

3. Scroll to the bottom of the file.

4. Change the IFW value from INFO to DEBUG as follows:

```
<!--
***************************************************************************
* Root logger definition
***************************************************************************
-->
    <!-- ROOT IFW LOGGER -->
    <logger name="com.ca.ssa.servicediscovery" additivity="false">
        <level value="INFO" />
                <appender-ref ref="SD" />
    </logger>
    <logger name="com.ca.ehealth" additivity="false">
        <level value="INFO" />
            <appender-ref ref="EH" />
    </logger>
     <logger name="com.ca.sam.ifw" additivity="false">
        <level value="DEBUG" />
            <appender-ref ref="IFW" />
    </logger>
    <logger name="com.ca.ucf" additivity="false">
        <level value="INFO" />
            <appender-ref ref="UCF" />
    </logger>
    <root>
        <level value="ERROR" />
        <appender-ref ref="ROOT" />
    </root>
```

5. Save the file.

   The changes are saved and the log level is set to DEBUG.

   Note: You do not need to restart anything for the changes to take effect or to create the debug files.

Generate an Alert in CA Spectrum to Forward to CA SOI

After you enable the debug, generate an alert in CA Spectrum. For this scenario, you create an alert in CA Spectrum by changing the community string on a device to generate a MANAGEMENT AGENT LOST alert.

Follow these steps:

1. Launch the CA Spectrum OneClick console.

2. Select the appropriate device and click the Information tab in the Component Detail panel.

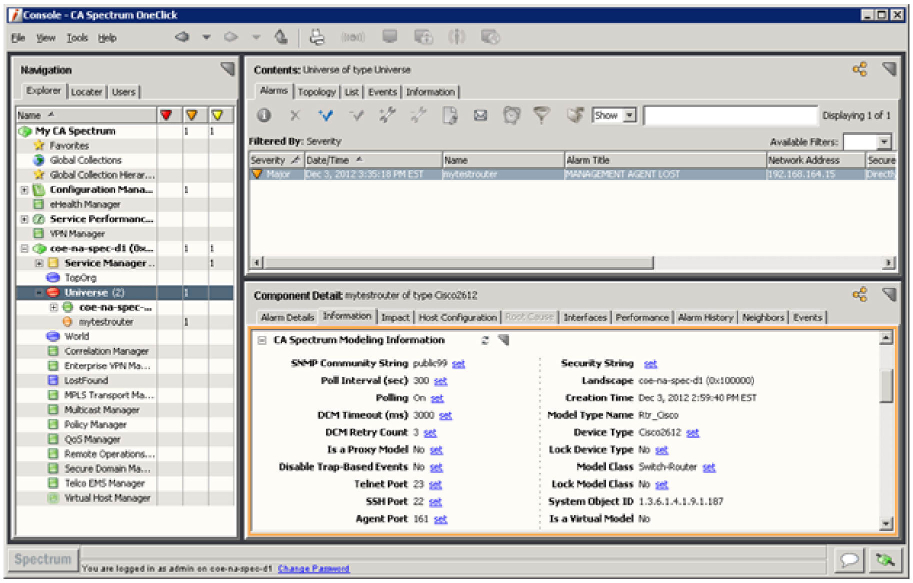
3. Navigate to the CA Spectrum Modeling Information section.

4. Click the *set* link next to SNMP Community String.

5. Add 99 to the end of the community string and press enter.

6. Right-click the device and select Poll to speed up the time it takes for the alert to appear in CA Spectrum OneClick.

7. Verify that your screen looks as follows (after the alert is created):



Contents: Universe of type Universe

Filtered By: Severity

Severity	Date/Time	Name	Alarm Title	Network Address	Secure
Major	Dec 3, 2012 3:35:18 PM EST	mytestrouter	MANAGEMENT AGENT LOST	192.168.164.15	Direct

Component Detail: mytestrouter of type Cisco2612

CA Spectrum Modeling Information

SNMP Community String	public99 set	Security String	set
Poll Interval (sec)	300 set	Landscape	coe-na-spec-d1 (0x100000)
Polling	On set	Creation Time	Dec 3, 2012 2:59:40 PM EST
DCM Timeout (ms)	3000 set	Model Type Name	Rtr_Cisco
DCM Retry Count	3 set	Device Type	Cisco2612 set
Is a Proxy Model	No set	Lock Device Type	No set
Disable Trap-Based Events	No set	Model Class	Switch-Router set
Telnet Port	23 set	Lock Model Class	No set
SSH Port	22 set	System Object ID	1.3.6.1.4.1.9.1.187
Agent Port	161 set	Is a Virtual Model	No

You are logged in as admin on coe-na-spec-d1

8. Verify that you can see the alert in CA Spectrum OneClick and CA SOI.

View Logs to Track the Flow of Alerts

To track the flow of the alert from CA Spectrum to CA SOI, view the debug RAW and PUB files:

1. View Alert_RAW File (see page 58).

2. View Alert_PUB File (see page 59).

View Alert_RAW File

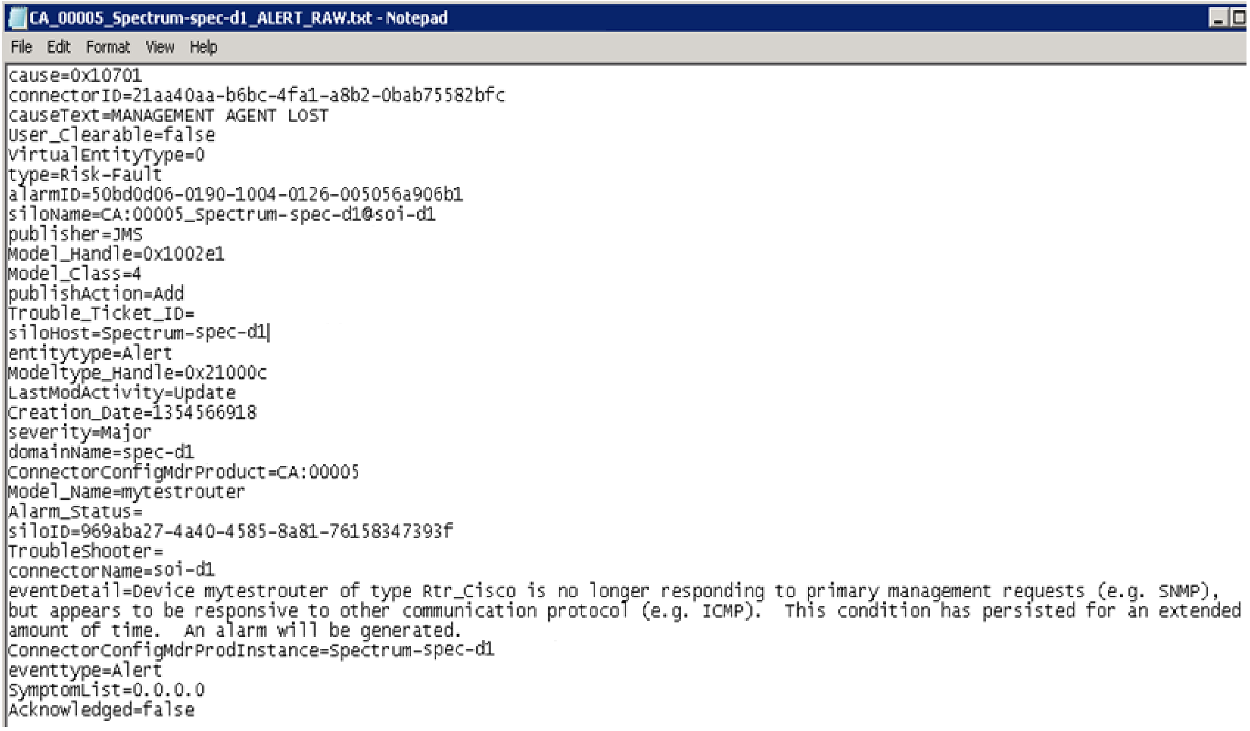
The Alert_RAW file contains *raw* alerts coming from CA Spectrum. The information in this file also signifies that the alert that was generated in CA Spectrum has been sent successfully to the CA Spectrum connector.

Therefore, if you see your particular alert in this file, it implies that the alert has been sent from CA Spectrum to the connector.

Follow these steps:

1. Navigate to the SOI_HOME\log\debugData folder on the server where the CA Spectrum connector is installed.
2. Open the CA_00005_Spectrum-<*SShostname*>_Alert_RAW.txt file.

   Note: *SShostname* specifies the host name of the CA Spectrum server.
3. Verify that the new MANAGEMENT AGENT LOST alert is present in the CA_00005_Spectrum-<*SShostname*>_Alert_RAW.txt file as shown in the following screenshot:


CA_00005_Spectrum-spec-d1_ALERT_RAW.txt - Notepad
File Edit Format View Help

```
cause=0x10701
connectorID=21aa40aa-b6bc-4fa1-a8b2-0bab75582bfc
causeText=MANAGEMENT AGENT LOST
User_Clearable=false
VirtualEntityType=0
type=Risk-Fault
alarmID=50bd0d06-0190-1004-0126-005056a906b1
siloName=CA:00005_Spectrum-spec-d1@soi-d1
publisher=JMS
Model_Handle=0x1002e1
Model_Class=4
publishAction=Add
Trouble_Ticket_ID=
siloHost=Spectrum-spec-d1
entitytype=Alert
Modeltype_Handle=0x21000c
LastModActivity=Update
Creation_Date=1354566918
severity=Major
domainName=spec-d1
ConnectorConfigMdrProduct=CA:00005
Model_Name=mytestrouter
Alarm_Status=
siloID=969aba27-4a40-4585-8a81-76158347393f
TroubleShooter=
connectorName=soi-d1
eventDetail=Device mytestrouter of type Rtr_Cisco is no longer responding to primary management requests (e.g. SNMP),
but appears to be responsive to other communication protocol (e.g. ICMP).  This condition has persisted for an extended
amount of time.  An alarm will be generated.
ConnectorConfigMdrProdInstance=Spectrum-spec-d1
eventtype=Alert
SymptomList=0.0.0.0
Acknowledged=false
```

View Alert_PUB File

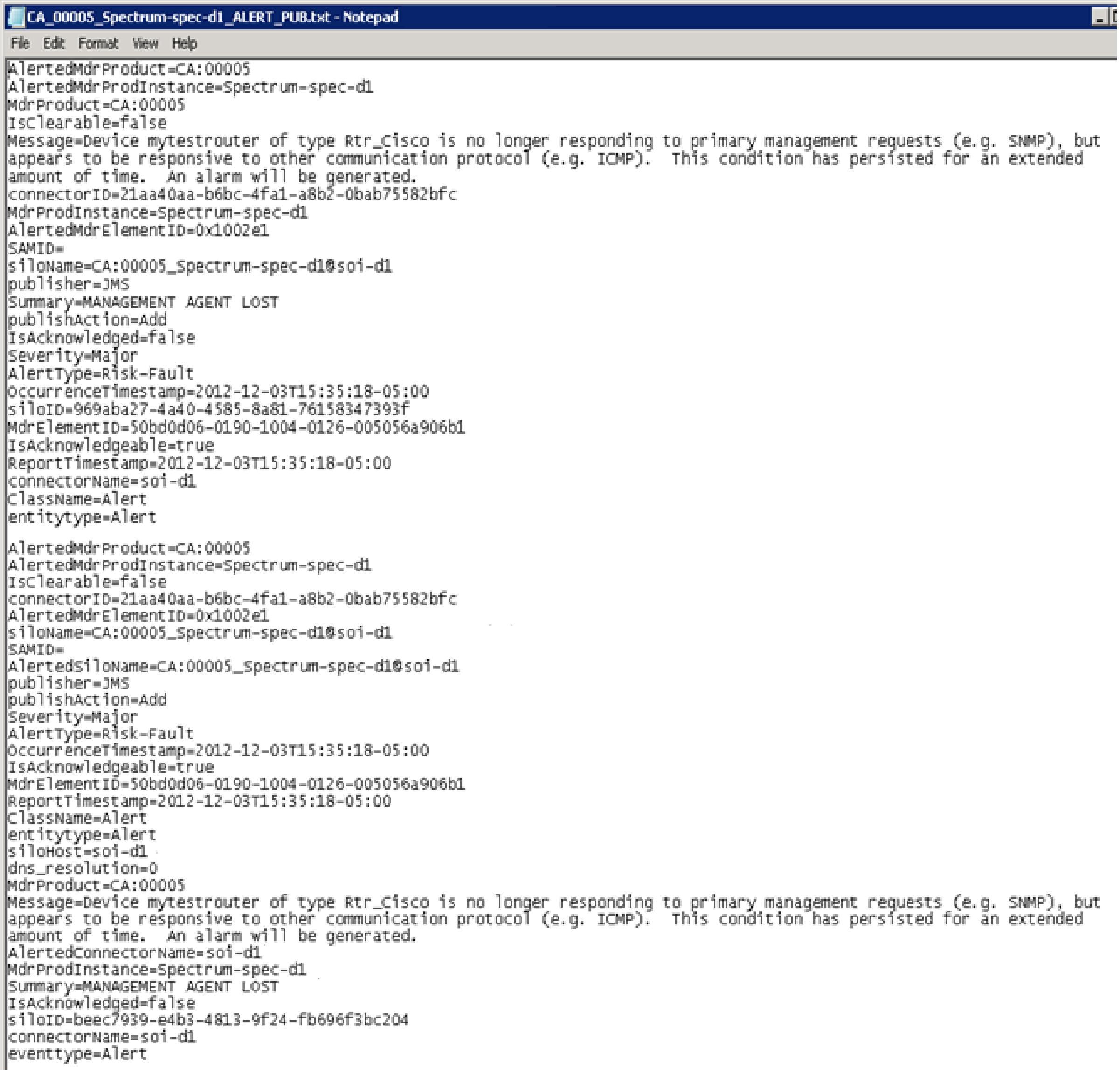
The information in the Alert_PUB file signifies that the alert that was in the Alert_RAW file has now been transformed using the USM properties. The details also imply that the alert has been sent to CA Catalyst and should show in the CA SOI Operations Console.

Follow these steps:

1. Navigate to the SOI_HOME\log\debugData folder on the server where the CA Spectrum connector is installed.
2. Open the CA_00005_Spectrum-<*SShostname*>_Alert_PUB.txt file.

   Note: *SShostname* specifies the host name of the CA Spectrum server.

3. Verify that the new MANAGEMENT AGENT LOST alert is present in the CA_00005_Spectrum-<*SShostname*>_Alert_PUB.txt file as shown in the following screenshot:



CA_00005_Spectrum-spec-d1_ALERT_PUB.txt - Notepad
File Edit Format View Help

```
AlertedMdrProduct=CA:00005
AlertedMdrProdInstance=Spectrum-spec-d1
MdrProduct=CA:00005
IsClearable=false
Message=Device mytestrouter of type Rtr_Cisco is no longer responding to primary management requests (e.g. SNMP), but
appears to be responsive to other communication protocol (e.g. ICMP).  This condition has persisted for an extended
amount of time.  An alarm will be generated.
connectorID=21aa40aa-b6bc-4fa1-a8b2-0bab75582bfc
MdrProdInstance=Spectrum-spec-d1
AlertedMdrElementID=0x1002e1
SAMID=
siloName=CA:00005_Spectrum-spec-d1@soi-d1
publisher=JMS
Summary=MANAGEMENT AGENT LOST
publishAction=Add
IsAcknowledged=false
Severity=Major
AlertType=Risk-Fault
OccurrenceTimestamp=2012-12-03T15:35:18-05:00
siloID=969aba27-4a40-4585-8a81-76158347393f
MdrElementID=50bd0d06-0190-1004-0126-005056a906b1
IsAcknowledgeable=true
ReportTimestamp=2012-12-03T15:35:18-05:00
connectorName=soi-d1
ClassName=Alert
entitytype=Alert

AlertedMdrProduct=CA:00005
AlertedMdrProdInstance=Spectrum-spec-d1
IsClearable=false
connectorID=21aa40aa-b6bc-4fa1-a8b2-0bab75582bfc
AlertedMdrElementID=0x1002e1
siloName=CA:00005_Spectrum-spec-d1@soi-d1
SAMID=
AlertedSiloName=CA:00005_Spectrum-spec-d1@soi-d1
publisher=JMS
publishAction=Add
Severity=Major
AlertType=Risk-Fault
OccurrenceTimestamp=2012-12-03T15:35:18-05:00
IsAcknowledgeable=true
MdrElementID=50bd0d06-0190-1004-0126-005056a906b1
ReportTimestamp=2012-12-03T15:35:18-05:00
ClassName=Alert
entitytype=Alert
siloHost=soi-d1
dns_resolution=0
MdrProduct=CA:00005
Message=Device mytestrouter of type Rtr_Cisco is no longer responding to primary management requests (e.g. SNMP), but
appears to be responsive to other communication protocol (e.g. ICMP).  This condition has persisted for an extended
amount of time.  An alarm will be generated.
AlertedConnectorName=soi-d1
MdrProdInstance=Spectrum-spec-d1
Summary=MANAGEMENT AGENT LOST
IsAcknowledged=false
siloID=beec7939-e4b3-4813-9f24-fb696f3bc204
connectorName=soi-d1
eventtype=Alert
```

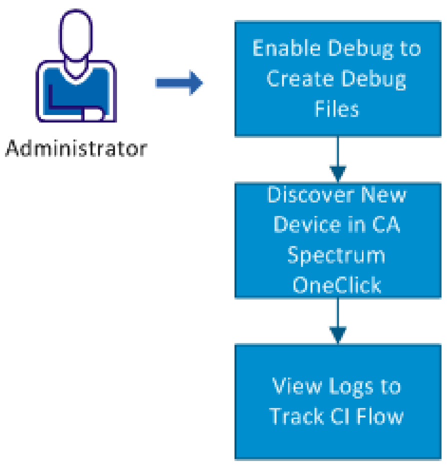
Therefore, an alert that was originally generated in CA Spectrum shows in the Alert_RAW file and the Alert_PUB file. This flow indicates that this alert was forwarded successfully from CA Spectrum to CA SOI and is now displayed in the CA SOI Operations Console.

How to Track CIs from CA Spectrum to CA SOI Using Debug Logs

As a CA SOI administrator, you can enable debug on the CA Spectrum connector and can investigate the debug logs to track CIs as they flow from CA Spectrum to CA SOI.

Use this scenario to guide you through the process:

How to Track CIs from CA Spectrum to CA SOI Using Debug Logs


Administrator
Enable Debug to Create Debug Files
Discover New Device in CA Spectrum OneClick
View Logs to Track CI Flow

1. Enable Debug to Create Debug Files (see page 55).

   Note: If the debug level is already set to DEBUG, do not perform this step. The steps are similar to the information already mentioned in the alert procedure.

2. Discover a New Device in CA Spectrum OneClick (see page 61).
3. View Logs to Track the Flow of CIs (see page 62).
   a. View ITEM_RAW File (see page 62).
   b. View CI_PUB File (see page 64).

Discover a New Device in CA Spectrum OneClick

Launch the CA Spectrum Oneclick console and discover a new device.

Note: For more information about working with the CA Spectrum Oneclick console, see the CA Spectrum documentation.

View Logs to Track the Flow of CIs

To track the flow of new CIs that are added to CA Spectrum into CA SOI, view the debug RAW and PUB files:

1. View ITEM_RAW File (see page 62).
2. View CI_PUB File (see page 64).

View ITEM_RAW File

The ITEM_RAW file contains *raw* details of the newly discovered device in CA Spectrum. The information in this file signifies that the device in CA Spectrum was sent successfully to the CA Spectrum connector.

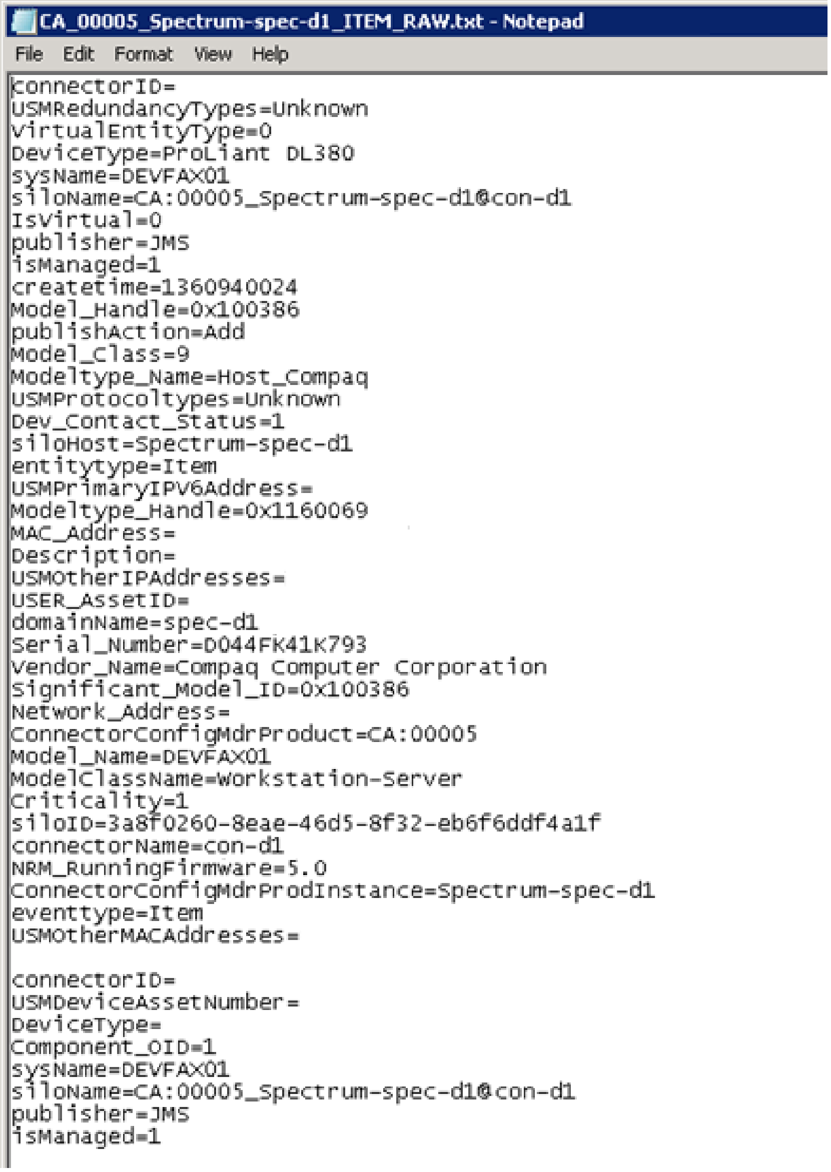
Therefore, if you see your particular device in this file, it implies that the device has been sent from CA Spectrum to the connector.

Follow these steps:

1. Navigate to the SOI_HOME\log\debugData folder on the server where the CA Spectrum connector is installed.
2. Open the CA_00005_Spectrum-<*SShostname*>_ITEM_RAW.txt file.

   Note: *SShostname* specifies the host name of the CA Spectrum server.

3. Verify that you see the details of the new device and its child CIs (such as interfaces and ports) in the ITEM_RAW file as shown in the following screenshot:


CA_00005_Spectrum-spec-d1_ITEM_RAW.txt - Notepad
File Edit Format View Help

```
connectorID=
USMRedundancyTypes=Unknown
VirtualEntityType=0
DeviceType=ProLiant DL380
sysName=DEVFAX01
siloName=CA:00005_Spectrum-spec-d1@con-d1
IsVirtual=0
publisher=JMS
isManaged=1
createtime=1360940024
Model_Handle=0x100386
publishAction=Add
Model_Class=9
Modeltype_Name=Host_Compaq
USMProtocoltypes=Unknown
Dev_Contact_Status=1
siloHost=Spectrum-spec-d1
entitytype=Item
USMPrimaryIPV6Address=
Modeltype_Handle=0x1160069
MAC_Address=
Description=
USMOtherIPAddresses=
USER_AssetID=
domainName=spec-d1
Serial_Number=D044FK41K793
Vendor_Name=Compaq Computer Corporation
Significant_Model_ID=0x100386
Network_Address=
ConnectorConfigMdrProduct=CA:00005
Model_Name=DEVFAX01
ModelClassName=Workstation-Server
Criticality=1
siloID=3a8f0260-8eae-46d5-8f32-eb6f6ddf4a1f
connectorName=con-d1
NRM_RunningFirmware=5.0
ConnectorConfigMdrProdInstance=Spectrum-spec-d1
eventtype=Item
USMOtherMACAddresses=

connectorID=
USMDeviceAssetNumber=
DeviceType=
Component_OID=1
sysName=DEVFAX01
siloName=CA:00005_Spectrum-spec-d1@con-d1
publisher=JMS
isManaged=1
```

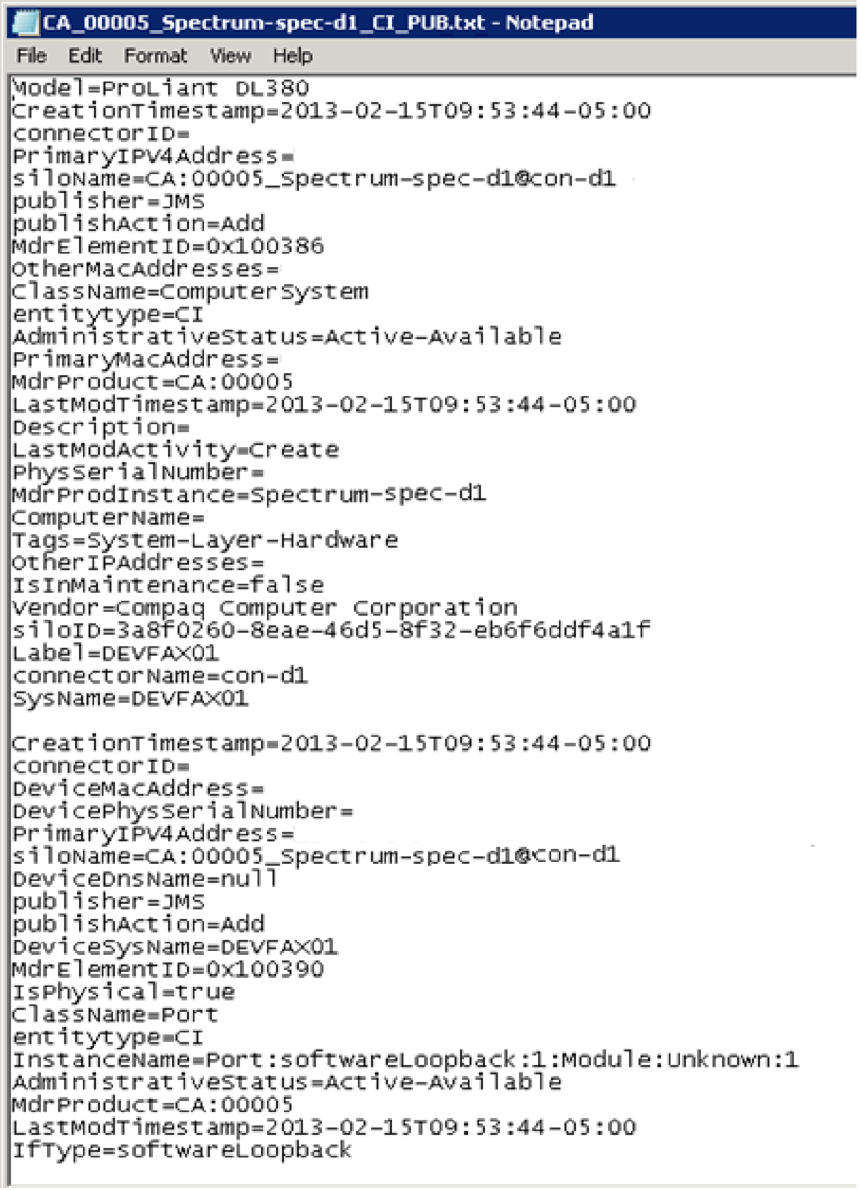
View CI_PUB File

The CI_PUB file contains details of the transformed CI and its child CIs. The information in the file signifies that the CI that was in the Item_RAW file has now been transformed using the USM properties. The details also imply that the CI has been sent to CA Catalyst and should show in the CA SOI Operations Console.

Follow these steps:

1. Navigate to the SOI_HOME\log\debugData folder on the server where the CA Spectrum connector is installed.
2. Open the CA_00005_Spectrum-<*SShostname*>_CI_PUB.txt file.

   Note: *SShostname* specifies the host name of the CA Spectrum server.
3. Confirm the presence of the new CI in the CI_PUB file as shown in the following screenshot:


CA_00005_Spectrum-spec-d1_CI_PUB.txt - Notepad
File Edit Format View Help

```
Model=ProLiant DL380
CreationTimestamp=2013-02-15T09:53:44-05:00
connectorID=
PrimaryIPV4Address=
siloName=CA:00005_Spectrum-spec-d1@con-d1
publisher=JMS
publishAction=Add
MdrElementID=0x100386
OtherMacAddresses=
ClassName=ComputerSystem
entitytype=CI
AdministrativeStatus=Active-Available
PrimaryMacAddress=
MdrProduct=CA:00005
LastModTimestamp=2013-02-15T09:53:44-05:00
Description=
LastModActivity=Create
PhysSerialNumber=
MdrProdInstance=Spectrum-spec-d1
ComputerName=
Tags=System-Layer-Hardware
OtherIPAddresses=
IsInMaintenance=false
Vendor=Compaq Computer Corporation
siloID=3a8f0260-8eae-46d5-8f32-eb6f6ddf4a1f
Label=DEVFAX01
connectorName=con-d1
SysName=DEVFAX01

CreationTimestamp=2013-02-15T09:53:44-05:00
connectorID=
DeviceMacAddress=
DevicePhysSerialNumber=
PrimaryIPV4Address=
siloName=CA:00005_Spectrum-spec-d1@con-d1
DeviceDnsName=null
publisher=JMS
publishAction=Add
DeviceSysName=DEVFAX01
MdrElementID=0x100390
IsPhysical=true
ClassName=Port
entitytype=CI
InstanceName=Port:softwareLoopback:1:Module:Unknown:1
AdministrativeStatus=Active-Available
MdrProduct=CA:00005
LastModTimestamp=2013-02-15T09:53:44-05:00
IfType=softwareLoopback
```

4. Verify that the new CI and its child CIs now show up in the CA SOI Service Modeler.

Therefore, a CI that was discovered in CA Spectrum shows in the Item_RAW file and the CI_PUB file. This flow indicates that this CI was forwarded successfully from CA Spectrum to CA SOI and is now displayed in the CA SOI Operations Console.

Trace a CI Using USM Web View for Diagnosing Synchronization Errors

As an administrator, you can USM Web View to view the current state of a CI as CA Catalyst views it. You can use the USM Web View interface to get the CA Catalyst notebook ID and use it for tracing purposes. For example, to troubleshoot synchronization issues, you can use the notebook ID in the CA Catalyst Trace UI (see page 67) and can track the flow of tracing for the specific notebook. You can use that information to determine which component (Reconciler, Sync Planner, and Sync Executor) is creating the error and then review the error details.

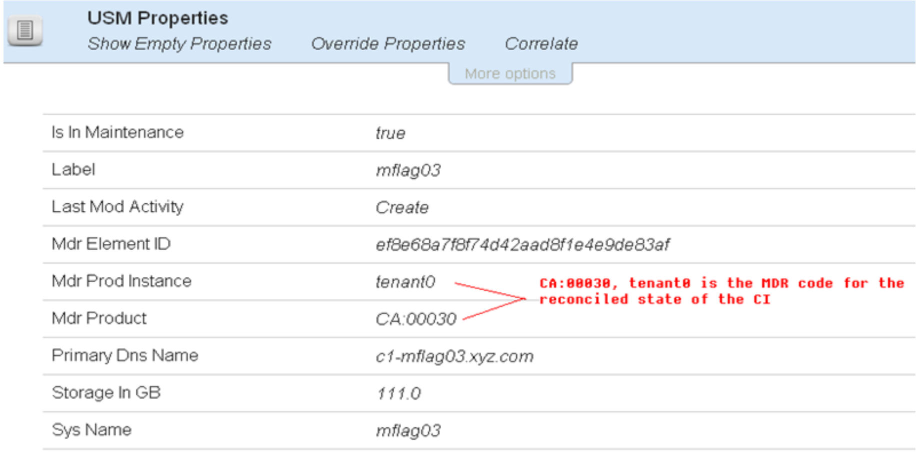
Follow these steps:

1. Open the CA SOI Dashboard and click the USM Web View link.

   The USM Web View interface opens.

2. Search for a known CI by entering a valid keyword (for example, label and sysname) value in the Search field.

3. View the USM Properties section that displays a reconciled view of the CI (for example, CA:00030, tenant0) by default. CA:00030, tenant0 is the MDR code for the reconciled state of the CI.



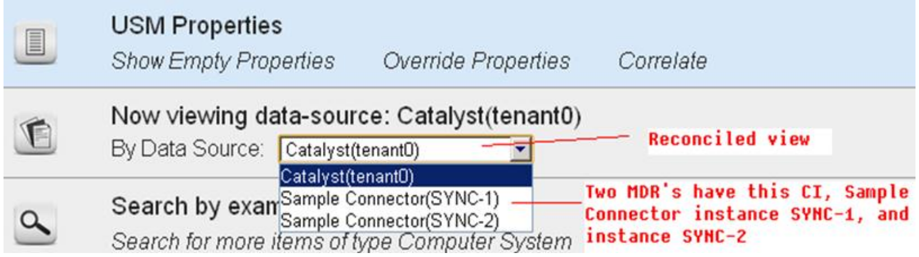
Is In Maintenance	true
Label	mflag03
Last Mod Activity	Create
Mdr Element ID	ef8e68a7f8f74d42aad8f1e4e9de83af
Mdr Prod Instance	tenant0
Mdr Product	CA:00030
Primary Dns Name	c1-mflag03.xyz.com
Storage In GB	111.0
Sys Name	mflag03

CA:00030, tenant0 is the MDR code for the reconciled state of the CI

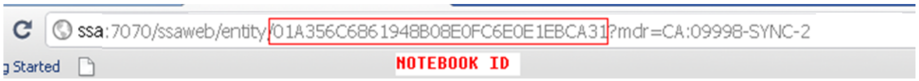
4. Click the More options link to display additional options.

5. Use the By Data Source drop-down list to get different projections of the CI.

6. Expand the drop-down list to see which domain managers are associated with the CI.



7. Review the URL to get the internal CA Catalyst notebook ID for tracing purposes. The notebook ID is embedded in the URL. In this example, the notebook ID is 01A356C6861948B08E0FC6E0E1EBCA31. You can use this notebook ID in the CA Catalyst Trace UI for further analysis.


ssa:7070/ssaweb/entity/01A356C6861948B08E0FC6E0E1EBCA31?mdr=CA:09998-SYNC-2
Started
NOTEBOOK ID

Use the CA Catalyst Trace UI for Diagnosing Synchronization Errors

As an administrator, use the CA Catalyst Trace UI to view the processing flow through the CA Catalyst components. The UI displays a list of actions that are performed by internal CA Catalyst components based on the notebook ID and transaction ID. A notebook ID represents the internal ID that CA Catalyst uses to reference a CI. A transaction ID represents a unique ID that is used to link together a sequence of operations that are performed on a CI. The entire processing flow shares the same transaction ID.

Note: For more information about the CA Catalyst Trace UI processing, see the CA Catalyst Trace UI Processing Flow (see page 68) section.

You can use the CA Catalyst Trace UI to determine what synchronizer is doing, whether it is succeeding or failing, and any reason for the failure. You filter the notebook ID in the UI and trace the processing flow to troubleshoot the error.

Follow these steps:

1. Enter the following URL in the web browser:

```
http://host:7090/sor.application/trace.jsp
```

host

Specifies the host name of the SA Manager server. For example, http://soi-server:7090/solr.application/trace.jsp.

The CA Catalyst Trace UI page displays.

2. Click the Reload Trace Log link.

   The trace log is reloaded.

3. Specify the notebook ID in the Filter field and click Submit Query.

   The UI shows only traces for the specific notebook.

   Note: For more information about how to find the notebook ID using USM Web View, see Trace a CI Using USM Web View for Diagnosing Synchronization Errors (see page 66).

4. Click the link in the Timestamp column to view the trace in more detail. For example, if the Action column shows the value as Error, you can click the corresponding timestamp value to view the exception that was encountered.

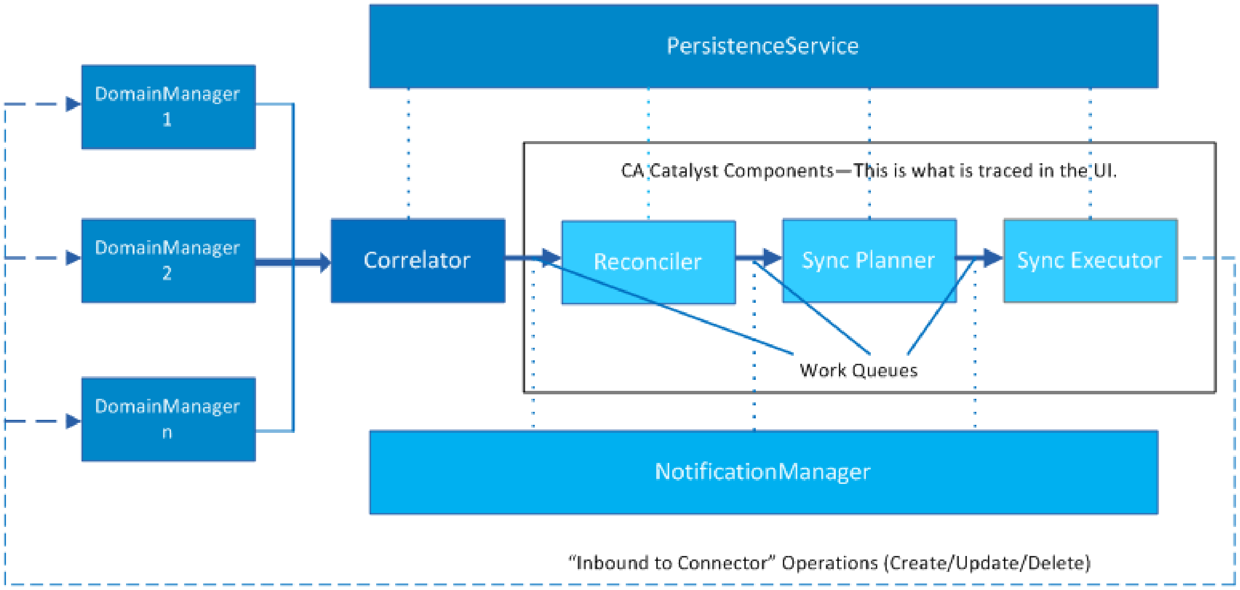
   The Trace details page opens and displays the detailed information.

5. Review the information.

CA Catalyst Trace UI Processing Flow

The following diagram shows the processing flow:

CA Catalyst Trace UI Processing Flow



The components in the diagram are explained as follows:

- Reconciler: Creates or updates the reconciled view of a CI.
- Sync Planner: Creates a synchronization plan based on the changes to the reconciled view.
- Sync Executor: Executes the synchronization plan.

The actions that are involved in the process are as follows:

- Dequeued: Specifies that the component has taken a notebook off the work queue for processing.
- Processed: Specifies that the component has completed working on the notebook.
- Error: Specifies that the component has encountered an error while trying to complete work on the notebook.
- Retry: Specifies that the component has decided to retry work on the notebook at a later time due to a recoverable error.
- Email: Specifies that the component has stopped trying to complete the work, either due to an unrecoverable error or because it has retried a maximum amount of time. By default, a component stops after retrying for 25 minutes, with a retry interval of 1 minute.

CA SOI Toolbox Utility

As an administrator, you use the CA SOI toolbox application to manage the maintenance of data in your CA SOI SA Store database. The toolbox is a command line utility which allows you to start and stop specific connectors and services, enabling efficient cleanups of your CA SOI instance.

The toolbox lets you clear unwanted data from your database. You can clear history data, imported data from connectors, and security data, individually or all at once.

The CA SOI toolbox is on the SA Manager in the SOI_HOME\Tools folder. Navigate to this location on a command prompt and run the following command with the options/parameters described in the ensuing sections:

```
soitoolbox
```

Note: The command help also contains information about the functions of the options and commands at are described in this section. For practical examples of using the utility, see How to Clean Up Data with the CA SOI Toolbox (see page 74).

Configuration Options

This section describes the different commands for the CA SOI toolbox that you can use to configure a CA SOI instance. In all commands, include the necessary options to establish a valid connection with the SA Store database. If you do not, the utility prompts you for the necessary information.

-m, --machine

Specifies the system to connect to which runs the SA Store database.

Default: localhost

-n, --mUsername

Specifies the name of the user who has access to the database system.

Note: This command is not valid and has no effect when using the localhost system.

Default: Administrator

-w, --mPassword

Specifies the password of the Windows users in plain text.

Note: This command is not valid and has no effect when using the localhost system.

-d, --dbName

Specifies the name of the CA SOI database.

Default: SAMStore

--dbArchiveName

Allows you to specify a new name for the archive database.

-u, --dbUsername

Specifies the user with privileges to access the CA SOI database.

Default: sa

-p, --dbPassword

Specifies the password for the database user in plain text.

Note: If the password is not specified, the utility requests it during runtime.

--credentials

Specifies the location of the file containing the user names and passwords for all systems that run CA SOI components. This command is required when you operate a distributed CA SOI instance.

-x

Creates a configuration file template if the file does not exist.

Note: This command is the equivalent of *--credentials=soitoolbox.cfg*.

-q, --quiet

Specifies that the user is not asked to confirm the running of a destructive operation.

-t, --timeout

Specifies the generic timeout in seconds.

Default: 30

-b, --dbConnectionTimeout

Specifies the timeout in seconds for the initial wait time for the opening of the database connection.

Default: 30

-c, --connector

Specifies the connectors to be used in action commands.

Default: *

Note: * in this case means all connectors in a CA SOI instance. The following examples show how the * symbol can be used:

```
--connector=CA:09998_soimachine.ca.com, CA:00005_soimachine.ca.com
--connector=CA:09998_*
--connector=CA:*_soimachine.ca.com
--connector=*
```

-s, --beSmart

Activates a special method for stopping connectors. In beSmart mode, the utility only stops components (services and connectors) which affect or can be affected by an action command.

Note: This option requires that you include --*credentials.*

Service Related Action Commands

You can use the following action commands to stop, start, and restart the services in a CA SOI instance. You can also use the utility to get information about the status of your services. The cleanup actions require the services to stop before the cleanup and restart after the cleanup. If you do not stop and restart the services, the utility performs the tasks automatically at the appropriate times.

These commands are:

--stopAllServices

Stops all the Windows services in a CA SOI instance.

--startAllServices

Starts all the Windows services in a CA SOI instance.

--restartAllServices

Restarts all the Windows services in a CA SOI instance by stopping and starting them.

--getServiceStatus

Displays the status of all the Windows services in a CA SOI instance.

Connector and Database Related Action Commands

Use the following action commands to manage and view the connector status. If you are cleaning up connector data, stop the connector before doing so.

--startConnector

Starts the connectors which you specify in the --*connector* parameter.

Note: Provide the --*credentials* parameter to use this command.

Important! If the CA SOI UI Server is not running, the command fails.

--stopConnector

Stops the connectors which you specify in the --*connector* parameter.

Note: Provide the --credentials parameter to use this command.

Important! If the CA SOI UI Server is not running, the command fails.

--getConnectorStatus

Provides the status of all the connectors in a CA SOI instance, including system connectors.

--getAvailableConnectors

Lists the names of all the connectors present in a CA SOI instance, excluding system connectors.

--getStatisticalData

Displays statistical data from the CA SOI database. This data includes information on the number of CIs, Alerts, and Services.

Note: The --*connector* option influences the output of this command.

Database Cleanup Commands

You can use the following commands to clean up the data in a CA SOI database.

--archiveHistoryData

Moves all historical data older than a specified number of days to an archive database.

Note: You specify the number of days by adding a number to the end of the command, for example --archiveHistoryData=10.

Note: The default name for the archive database is SOIArchiveDB. You can change the name of the archive database with the --*dbArchiveName* command.

--cleanHistoryData

Deletes all the historical data from the CA SOI database that is older than a specified number of days.

Note: You specify the number of days by adding a number to the end of the command which specifies the number of days.

--cleanImportedData

Deletes all the data that came from connectors that you specify in the --*connector* parameter.

Note: This command does not delete data that users create manually.

--cleanSecurityData

Deletes all service access rights that are set for specific users and groups within the CA SOI instance.

--cleanData

Deletes all history data, imported data, and security data for all the connectors in a CA SOI instance.

--purgeClearedAlerts

Deletes cleared alerts from the database that are older than a specified number of days. You can specify two different purge types, :*full* or :*strict*, by adding *full* or *strict* to the end of the command:

:full

Deletes all alerts that are cleared in at least one system.

:strict

Deletes only those alerts which are cleared in all systems.

--rebuildIndexes

Rebuilds database indexes.

--reinitializeDB

Clears the whole CA SOI database, deleting the data from all the tables.

Note: You can use this command to start with a clean state similar to that of a new installation.

--restoreHistoryData

Restores from the archive database all archived historical data that are not older than the specified number of days.

Note: You specify the number of days by adding a number to the end of the command, for example --restoreHistoryData=10.

How to Clean Up Data with the CA SOI Toolbox

As an administrator, you maintain the CA SOI database. You ensure that your database runs efficiently and that the data it maintains is the data you need. Using the CA SOI Toolbox command utility, you can clean up the following data types:

- Imported data from a specific connector
- History and security data
- All the data that is maintained in a CA SOI instance

You may want to clean up data for the following reasons:

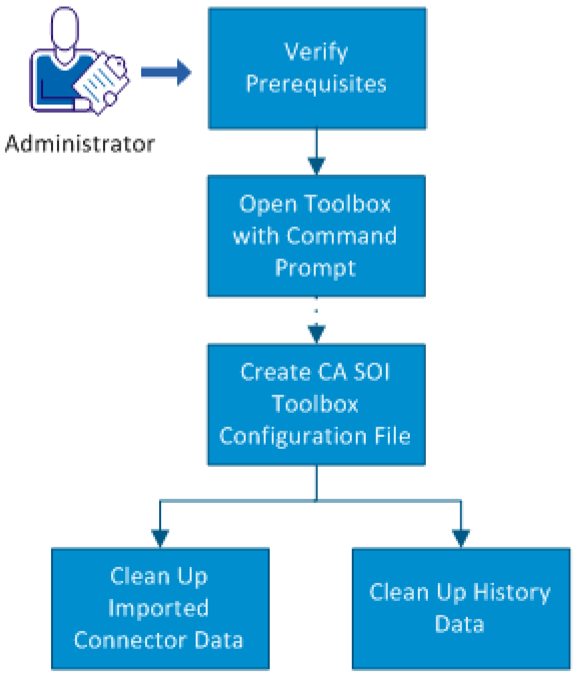
- You want to clean up data from a connector in your CA SOI instance that was not written correctly. Thus, the connector provides flawed data (for example, CIs using incorrect naming conventions) that does not correlate with data provided from other connectors.
- You want to maintain a more efficient CA SOI instance that does not maintain history that you do not need and consumes needed disk space. Thus, you clean up the history data that is no longer of use.

- Clear all security data for all users and user groups in a CA SOI instance.
- You want to restart a CA SOI instance from a clean state and clear all its data. This option is useful during the product implementation phase when incorrect connector configurations can cause database *pollution*.

Note: This scenario provides examples of commands for removing connector and history data. For detailed definitions of every parameter available, see the command help that comes with the toolbox.

Use this scenario to guide you through the process:

How to Clean Up Data with the CA SOI Toolbox


Administrator
Verify Prerequisites
Open Toolbox with Command Prompt
Create CA SOI Toolbox Configuration File
Clean Up Imported Connector Data
Clean Up History Data

1. Verify the prerequisites.
2. Determine the database sizing (see page 76).
3. Open the toolbox with a command prompt (see page 79).
4. (Optional) Create a CA SOI Toolbox configuration file (see page 80).
5. Do any of the following:
   - Clean up the history data (see page 81).
   - Clean up imported connector data (see page 82).

CA SOI Toolbox Prerequisites

To use the CA SOI toolbox, you must have the following information:

- The server credentials for the CA SOI instance
- The database location and credentials for the CA SOI instance if the database location is on a remote system

  Note: If you run an instance all on one server locally, you do not need credentials for the database.

- The name of the connector, If you want to perform a connector-specific cleanup

System Requirement:

- The CA SOI Toolbox requires that your system has the Microsoft Visual C++ 2008 Redistributable Package (x86) installed.

Determine Database Sizing

Maintaining the SA Store database is required to sustain consistent performance and maintain product function. Use the data provided in this section that is measured against the disk space and performance capabilities of your database server. You can then determine how often to perform maintenance.

The following tables display estimates of how you can expect the database to grow over time. They project growth over a three-year period for several implementation sizes.

Note: All tables assume that you have defined an SLA for every managed service.

Small (100 services, 1000 alerts per day)

Item	Amount	Average Row Size (KB)	Number of Rows	Disk Space Requirement (MB)
Managed CIs	20,000	.85	60,000	51
Staged CIs	100,000	1.345	300,000	403.5
Alerts	1,095,000	.6	3,285,000	1,971
Alert History		1.062	2,190,000	2,325.78
SLA	100	.3	109,500	32.85
History tables		.65	5,256,000	3,416

Item	Amount	Average Row Size (KB)	Number of Rows	Disk Space Requirement (MB)
Total table size				8,201
Database log file				4,920
Total size				13,121

Mid-sized (500 services, 5000 alerts per day)

Item	Amount	Average Row Size (KB)	Number of Rows	Disk Space Requirement (MB)
Managed CIs	50,000	.85	150,000	127.5
Staged CIs	500,000	1.345	1,500,000	2,018
Alerts	5,475,000	.6	16,425,000	9,855
Alert History		1.062	10,950,000	11,629
SLA	500	.3	547,500	164.25
History tables		.65	26,280,000	17,082
Total table size				40,875
Database log file				24,525
Total size				65,400

Large (1,000 services, 10,000 alerts per day)

Item	Amount	Average Row Size (KB)	Number of Rows	Disk Space Requirement (MB)
Managed CIs	100,000	.85	300,000	255
Staged CIs	1,000,000	1.345	3,000,000	4,035
Alerts	10,950,000	.6	32,850,000	19,710
Alert History		1.062	21,900,000	23,258

Item	Amount	Average Row Size (KB)	Number of Rows	Disk Space Requirement (MB)
SLA	1,000	.3	1,095,000	328.5
History tables		.65	52,560,000	34,164
Total table size				81,750
Database log file				49,050
Total size				130,800

Review the following considerations when interpreting these estimates:

- The Amount column lists the actual amount of each entity in CA SOI at the end of the three-year period. The Number of Rows column is larger than the actual amount in most cases.
- The SA Store tables not represented in this table are small enough that they have a negligible impact on database size.
- The History table row calculation is based on the fact that the three history tables (DBAvailHistory, DBQualityHistory, and DBRiskHistory) create a row every thirty minutes per service. Therefore, the history tables generate 48 rows per day per service.
- Plug your numbers into the table (total number of managed and staged CIs, average alerts received per day, and number of SLAs defined) that most closely approximates your implementation size to calculate the projected database growth rate for your implementation.
- The database log file is approximately 60 percent of the total database size.

Based on this data, you can make the following assumptions:

- At the end of a three-year period, the total disk space consumed by the SA Store database would be between 10,000-100,000 MB or 10-100 GB depending on the number of managed services, CIs, and alerts.
- You can expect a growth rate of roughly 2.7 GB per 1000 services per month, or 1.35 GB per 500 services per month, or 270 MB per 100 services per month.
- Consider these estimates when planning the frequency of maintenance to help ensure that the SA Store does not grow to an unmanageable size. As a best practice, the row count for all tables should be limited so that SQL queries on any table can complete within a few seconds. For example, if you find that this limit is around 10,000,000 rows per table on your database server, you would have to at least archive and purge the history tables periodically depending on implementation size to keep them from growing beyond this threshold.

Open the Toolbox with a Command Prompt

To use the toolbox to run its commands, open the toolbox with a command prompt.

Follow these steps:

1. Navigate to the CA SOI toolbox on the SA Manager in the <SOI_Home>\Tools folder.
2. Run the following command from the command prompt:

   ```
   soitoolbox
   ```

   The toolbox file opens in the command window and lists all the commands of the toolbox in the command help.

   Note: The following steps of this scenario provide two examples of different ways you can use the toolbox to clean up data.

Create a CA SOI Toolbox Configuration File

For CA SOI instances that do not run entirely in one local location, create a CA SOI toolbox configuration file. This configuration file allows you to run commands, using the -*x* option. The -*x* option allows you to provide all the credentials of a complex CA SOI instance which is not run in one location locally. To allow the running of commands using the -*x* option for a complex CA SOI instance, create a CA SOI toolbox configuration file.

Follow these steps:

1. Open the toolbox with a command prompt (see page 79).
2. Run the -*x* command from the toolbox.

   The toolbox creates an empty configuration file.

   Important! Before the toolbox creates the empty configuration file, an *ERROR: bad content - File not found* message appears. Disregard this message.
3. Open the empty configuration file *soitoolbox.cfg* in a text editor.

   The empty configuration file, which is a template, opens displaying instructions with placeholders.
4. Specify all the information for your CA SOI instance in the configuration file placeholders.

   Note: The file contains instructions about the information that you specify.
5. Save the configuration file with the changes you made.

   Your CA SOI instance now has a toolbox configuration file which you can use to run toolbox commands by using the -*x* option.

Note: Include the -*x* option before any call or command instead of specifying specific credentials when using the CA SOI toolbox. For example, you would run the following command to get a list of all the connectors in CA SOI instance after you set up the configuration file:

```
soitoolbox -x --getAvailableConnectors
```

Important! If you use the -*x* option, do not use the -*m* option to specify a machine. If you use both options in a command, an error occurs.

Clean Up History Data

When history data is no longer useful and you do not want to store in your database, you can clean up the history data. Maintenance of history data is important, because the history data can increase over time and can consume memory, thus adversely affecting the operation of the database. You can avoid buildup of unwanted data by cleaning up history data at regular intervals. With this command, you clean data which is older than a specified number of days. To clear unwanted history data in a database, run a cleanup command from the toolbox folder on a command prompt.

Follow these steps:

1. Open the toolbox with a command prompt (see page 79).
2. Run the history cleanup command and specify the database connection password. For example, if your database connection password is *yourpw*, and you want to delete history data that is older than 2 days, you would run:

   ```
   soitoolbox -p yourpw --cleanHistoryData=2
   ```

   -p

   Specifies the password. In this example, the password is *yourpw.*

   --cleanHistoryData

   Runs the command for deleting history data.

   2

   Specifies that only history data that is older than two days is deleted.

   The toolbox confirms that it found the services, connects to the database, and warns that you selected a destructive operation.

   Important! The example command assumes that your CA SOI instance runs entirely on a local system. If you are running a CA SOI instance that is not located entirely in one location, create a toolbox configuration file. For information about creating the toolbox configuration file, see Create a CA SOI Toolbox Configuration File (see page 80).

3. When prompted, confirm the destructive operation by typing Y for Yes.

   The toolbox verifies that CA SOI is running, and then asks you to stop the services before proceeding.

4. Confirm that you want to stop the services by typing Y for Yes.

   The toolbox stops the services and then deletes all the history data in the database.

5. Verify that the imported connector data was deleted by running the *--getStatisticalData* command.

   The toolbox returns information about the statistical data for the connector, confirming that the history data was deleted.

Clean Up Imported Connector Data

When a connector provides data that you do not want to store in your database, you can clean up data from the connector. To clean up imported connector data, run a cleanup command from the toolbox folder on a command prompt.

Follow these steps:

1. Open the toolbox with a command prompt (see page 79).
2. Run the cleanup command with the information about the connector name location and the location of the database where the connector data is stored.

   For example, if you wanted to delete data from the connector *Example_con* stored in a database that resides on the server *server1* with the database connection password *yourpw*, you would run:

   ```
   soitoolbox -p yourpw -m server1 --cleanImportedData --connector=Example_con
   ```

   The toolbox confirms that it found the services, connects to the database, and warns that you selected a destructive operation.

   Important! The example command assumes that your CA SOI instance runs entirely on a single server, *server1* in this case. If you are running a CA SOI instance that is not located entirely in one location, create a toolbox configuration file. For information about creating a toolbox configuration file, see Create a CA SOI Toolbox Configuration File (see page 80).

   Note: If you do not know your connector name, run the --*getAvailableConnectors* command first.

3. When prompted, confirm the destructive operation by typing Y for Yes.

   The toolbox verifies that SOI is running, and then asks you to stop the services before proceeding.

4. Confirm that you want to stop the services by typing Y for Yes.

   The toolbox stops the services and then deletes the imported connector data in the database.

5. Verify that the imported connector data was deleted by specifying the connector name with the --*connector* option and running the --*getStatisticalData* command.

   The toolbox returns information about the statistical data for the connector, confirming that the data was deleted.

   Note: If you are cleaning up data from a connector that is providing incorrect data, fix the connector problems before restarting its services.

Chapter 3: Troubleshooting

This section contains troubleshooting information for common problems categorized by CA SOI component.

This section contains the following topics:

Important! Before Troubleshooting a Problem (see page 83)
CA Catalyst Troubleshooting (see page 83)
Connectors Troubleshooting (see page 90)
Dashboard Troubleshooting (see page 105)
Event Management Troubleshooting (see page 108)
Help Desk Integrations Troubleshooting (see page 116)
Integration Framework Troubleshooting (see page 119)
Mobile Dashboard Troubleshooting (see page 120)
Operations Console Troubleshooting (see page 121)
SA Manager and UI Server Troubleshooting (see page 129)
SOI Toolbox Troubleshooting (see page 133)
USM Web View Troubleshooting (see page 133)

Important! Before Troubleshooting a Problem

Before you troubleshoot any problem in this section, run the Triage Tests on the SA Manager Server (see page 17) and the UI Server (see page 19). The Triage Tests help you diagnose major problems in the system. Many minor problems that you experience can be the result of a much greater problem in the system.

If any Triage Test fails, resolve the Triage Test failure problem before attempting to resolve any other issue.

Once all Triage Test problems are resolved, then continue to the other troubleshooting topics in this chapter.

CA Catalyst Troubleshooting

The troubleshooting topics in this section relate to CA Catalyst.

Synchronization - Priming Utility Runs for Hours

Symptom:

I ran the priming utility to perform a full synchronization to the realtime environment. The utility ran for hours without finishing.

Solution:

As a best practice, synchronize the CI types first then relationships. For synchronization procedures, see the *Administration Guide*.

Depending your system and the number of CIs, the priming utility can run for hours or days before completing synchronization.

Also, while the priming utility runs, CA SOI typically appends many “ObjectNotFound” exceptions in the SA Manager log. The exceptions occur because CA SOI does not enforce sequencing of items and relationships. Therefore, CA SOI can process the relationships before the reconciled sheets are created for the parent, child, or relationship scope.

Installation or Initialization Errors

Symptom:

You experience installation errors or have problems initializing CA Catalyst components. The specific problems can include the following:

- Components do not install correctly.
- The Registry is inaccessible.
- SA Manager or IFW does not start.
- UCF failed.

Solution:

Try the following solutions to resolve common installation or initialization problems:

- Check the installation logs at SOI_HOME\log. The following log files are available for debugging CA Catalyst components at SOI_HOME\log:
  - CA-SSA-LogicInstallDebug.log
  - CA-SSA-RegistryInstallDebug.log
  - ucf.log
- Check the following services and ensure that they are all started:
  - CA SAM Application Server
  - CA SAM Integration Services

  - CA SAM Store Indexer
  - CA SAM User Interface Server
  - CA UCF Broker

  Note: For more information about using services for diagnosis, see Using Services for Diagnosis (see page 35).

- Check the services logs at SOI_HOME\jsw\logs if a service does not start.
- Check the CA SOI error logs if problems persist. CA Catalyst components run under the SA Manager, so problems with this and other CA SOI components can affect CA Catalyst components.
- For IFW problems not caused by a service failure, check the SOI_HOME\log\ifw.log file for errors. Verify the appropriate IFW configuration in the SOI_HOME\resources\Configurations\SSA_IFW_*servername*.xml file.

Note: For more information about using log files for diagnosis, see Using Log Files for Diagnosis (see page 20).

ActiveMQ Server Errors

Symptom:

The ActiveMQ server must be operating properly for information to make it to the Logic Server. Problems with all CA Catalyst components can originate in the ActiveMQ server. The following problems can occur:

- ActiveMQ not started
- ActiveMQ connectivity problems

Solution:

Perform the following actions to resolve the errors:

- Check the SOI_HOME\tomcat\logs\soimgr-error.log file for errors that are related to ActiveMQ startup.
- Check the ActiveMQ log file for errors.
- Verify that activemq-web.war is deployed.
- Verify the ActiveMQ configuration in the SOI_HOME\tomcat\webapps\activemq-web\WEB-INF\caifwmq.xml file.
- Verify that the ActiveMQ connection information is correct in all appropriate configuration files.
- Verify the ActiveMQ topic and queue permissions.

Registry Errors

Symptom:

You experience errors with Registry functionality, such as the following issues:

- Problems connecting to the SA Store database
- Cannot access Registry
- Registry content missing
- The sor.application program within the Registry is not starting

Solution:

Try the following solutions to fix Registry errors:

- Verify that the SA Store database credentials in the SOI_HOME\ws02registry\repository\conf\registry.xml file are correct.
- Access problems can be caused by invalid credentials or an unencrypted password that is stored in the Registry. If you cannot access the Registry, check the credentials in the ssaserver.xml and sorapp.xml files at SOI_HOME\tomcat\registry\topology\physical\node0\sor.
- If Registry content is missing, check the database credentials in the sorapp.xml and ssaserver.xml file.
- Check the SOI_HOME\tomcat\registry\topology\logical\tenant0\usmschema folder and verify that the following files exist:
  - addressing.xsd
  - sml.xsd
  - usm-core-200907.xsd
  - usm-query.xml
  - usm-elemconstraints.xml
  - usm-extensions-201001.xsd
  - usm-infradefaults.xml
  - usm-metadata-200907.xsd
  - usm-metrics-200907.xsd
  - usm-openenums.xml

  If these files do not exist or are corrupted, the USM schema did not install correctly.
- If sor.application does not start, check the topology\physical\node0\sorappbootstrap.xml file and verify that it correctly points to the sorapp.xml file. Also, verify that sor.application.war is deployed.

Correlation and Persistence Errors

Symptom:

You experience errors with the correlation and the information added to the database by the Persistence Service, which can include the following issues:

- No notebooks created
- No projection sheets created
- Correlation did not occur
- Missing correlated events

Solution:

Try the following solutions:

- Verify that the SA Manager is initialized.
- Verify that the Persistence Service is initialized.
- Verify that the Notification Manager is initialized with the correct configuration.

Notification Manager Errors

Symptom:

You experience problems with correlation or other functions, and log file investigation pinpoints the Notification Manager as the source of the problem. The Notification Manager must be initialized and configured correctly.

Solution:

Try the following solutions:

- Verify that the ActiveMQ server is initialized.
- Verify that the following topics are defined in the sorapp.xml and ssaserver.xml files:
  - PlansToBeApproved
  - SynchronizationPlans
  - ReconciledSheets
  - InstructionQueue
  - CorrelatedNotebooks

Reconciliation Errors

Symptom:

You experience errors that are related to the reconciliation, which include the following issues:

- Outbound from connector operations failed
- No reconciled sheet is created
- Reconciler does not initialize

Solution:

Try the following solutions:

- Verify that all components installed and initialized properly.
- Verify the correct operation of the correlation and Persistence Service components.
- Verify that reconciliation policy is configured correctly. Verify the existence of the defaultsheet.xml file in the Registry and the Reconciler contents in the sorapp.xml and ssaserver.xml files.

Synchronization Errors

Symptom:

You experience problems with the synchronization functionality. Synchronization errors usually appear as failed inbound to connector operations or mismatches between projections and reconciled sheets. Synchronization errors may be caused by the following issues:

- Sync Planner failed
- Sync Executor failed
- Synchronization not enabled

Solution:

Try the following to fix synchronization errors:

Review the "Working with CA Catalyst Synchronization" section in the *Administration Guide*. The section provides detailed information about making sure that everything is configured correctly from the connector configuration to UCF Broker to CA Catalyst registry.

- Verify that the Synchronizer is enabled. Enabling the maintenance mode synchronization automatically enables the Synchronizer.

- Verify that the connector to which you are trying to synchronize is configured properly. Open the CA SOI Administration UI, select the connector, and review the following information:
  - In the Connector Controls section, verify that the isRemotable connector control is enabled.
  - In the InboundToConnectorTypes section, verify that a list of all USM types that are supported for synchronization exists. To synchronize on a particular CI, its type must be included in the list.
- Verify the correct location of the UCF Broker.

  Note: For more information about how to configure the UCF Broker location, see the *Administration Guide*.
- Verify that all applicable connectors support inbound to connector operations.
- Verify that all connectors have inbound to connector operations enabled.
- Verify that sor.application started correctly.
- Verify that the CI on which synchronization is required has been reconciled with CA SOI. Check for mismatches between projections and reconciled sheets using the USM Web View interface:
  - Find the reconciled view of the CI in USM Web View (for example, CA:00030, tenent0).
  - Get different projections for the CI using the *By Data Source* drop-down list.

  Note: For more information about these points, see Trace a CI Using USM Web View for Diagnosing Synchronization Errors (see page 66).
- Verify that the Synchronizer is executing the synchronization transactions.
  - Get the internal CA Catalyst notebook ID for the CI using the USM Web View interface.
  - Use the CA Catalyst Trace UI (see page 67) (http://*host*:7090/sor.application/trace.jsp) to track events on the notebook using the notebook ID.
- Review the related log file. CA Catalyst uses log4j for logging. By default, only Errors and Warnings are logged to the SOI_HOME\tomcat\logs\soimgr.log file. Enable the debug logging in CA Catalyst by editing the SOI_HOME\tomcat\lib\log4j.xml file. Update the existing logger entry in the file by changing the debug level from “INFO” to “DEBUG” and restart the CA SAM Application Server service:

```
<logger name="com.ca.ssa.sor" additivity="false">
    <level value="DEBUG" />
    <appender-ref ref="CAT" />
</logger>
```

CA Catalyst debug log entries start appearing in the soimgr.log file.

Failures can also occur in connectors when fulfilling the update request. Review the individual connector logs to view the request and any errors that occur.

Connectors Troubleshooting

The troubleshooting topics in this section relate to connectors in general. For information related to specific connectors, see the respective *Connector Guide* provided with the connector.

Alert Synchronization Not Working for a Connector

Symptom:

I am trying to implement alert synchronization (*inbound to connector* operation) for my connector, but it is not working. How do I troubleshoot this issue?

Solution:

For *inbound to connector* synchronization, the update() method of connectors is called with the alert details. If the update() method is not getting called, this problem usually means an issue in either the connector configuration or CA Catalyst synchronizer policy. To troubleshoot, perform the following steps:

- Verify that the connector is enabled for the inbound to connector operations. To do so, verify that the value of the *isRemotable* connector control is set to 1 in the connector configuration file.
- Verify that the connector is exposing *Alerts* as a supported USM type for synchronization (*inbound to connector*). You can do so by verifying that the connector configuration file has *Alert* listed under *InboundToConnectorTypes*.
- Enable CA Catalyst synchronizer from the CA SOI Administration UI.
- The default synchronization policy that is shipped with the product enables synchronizations (inbound to connector) for a specific connector or (domain manager). You may need to add your connector to this list as follows:
    1. Open the SOI_HOME\tomcat\registry\topology\physical\node0\sor\syncfilters\alert_filter.xml file in a text editor.
    2. Add your domain manager product identifier (for example, CA:01234) to the list of domain managers in the file.

An example is provided as follows:

```
<action defaultBehavior="drop">
  <send>
    <mdr productName="CA:00003" /> <!-- NSM-DSM -->
     <mdr productName="CA:00005" /> <!-- SPIM -->
     <mdr productName="CA:00031" /> <!-- SCOM -->
     <mdr productName="CA:01234" /> <!— Your connector -->
  </send>
 </action>
```

3. Reload the registry and restart the CA SAM Application Server service for the change to take effect.

CA Spectrum Connector Binding in a Dual NIC Environment

Symptom:

CA Spectrum alerts (through the CA Spectrum connector) are not showing up in CA SOI in an environment that uses dual NIC servers.

Solution:

On dual NIC servers, binding order on both CA Spectrum connector and CA Spectrum servers needs to be correct, and must bind to the same NIC.

CA Spectrum must not bind to the secondary, non-routable IP address on the connector server. Setting the proxy host can help in this dual NIC case when the CA Spectrum server can only connect to one of the two IPs/FQDNs for the connector server.

As a workaround, hard code the primary IP address of the correct NIC in the SOI_HOME\jsw\conf\SAM-IntegrationServices.conf file on the connector server. For example:

wrapper.java.additional.*number*=-Dvbroker.se.iiop_tp.host=

wrapper.java.additional.*number*=-Dvbroker.se.iiop_tp.proxyHost=*proxyhostname*

proxyhostname in this case is the local IP or hostname that the remote server can use to connect back.

CA Spectrum Connector Keeps Reinitializing

Symptom:

After I have installed CA Spectrum in a Microsoft Cluster Server environment, the CA Spectrum connector fails to start (it keeps reinitializing).

Solution:

Each node in the cluster must have at least two network adapters. One adapter is used for the client public network and the second one is used for internal cluster communication.

If the order of adapters and bindings is wrong, the CA Spectrum connector fails to start. The adapter for public network must be listed first in the Adapters and Bindings list in Windows Network Connections Advanced Settings.

CA Spectrum Connector Firewall Limitations

Symptom:

CA Spectrum alerts are not showing up in CA SOI (after connector initialization) in an environment that uses a firewall between the CA Spectrum server and CA Spectrum connector.

Solution:

If the firewall exists between the CA Spectrum server and CA Spectrum connector, the CA Spectrum connector uses a random listener port (instead of the bidirectional static port) to communicate with the CA Spectrum server to receive callbacks. Because of this reason, no new alerts are passed on to CA SOI after the connector initialization phase.

As a workaround, hard code the listener port on the connector server to a static port (for example, 14001) in the SOI_HOME\jsw\conf\SAM-IntegrationServices.conf file, and open the port bidirectionally on the firewall. For example, wrapper.java.additional.*number*=-Dvbroker.se.iiop_tp.scm.iiop_tp.listener.port=14001. This port has to be open from the CA Spectrum server to the connector server.

Change Connector Credentials

Symptom:

How do I change the username and password for a connector?

Solution:

You can change the username and password in the respective connector configuration file.

Follow these steps:

1. For each connector, the configuration file is located in the following folder:

   SOI_HOME\resources\Configurations\*connectorname_hostname*.xml

2. Open the configuration file for editing.
3. Locate the username and password fields.

   Because the password is encrypted, you next run the encryption utility.

4. Open a command line and locate the encryption utility in the following folder:

   SOI_HOMEI\Tools\EncryptSAMCreds.bat

5. Run the following command:

   ```
   EncryptSAMCreds.bat password_to_encrypt
   ```

6. Copy and paste the encrypted password in the properties file password field.
7. Save the properties file.
8. Restart the CA SAM Integration Services service to implement the changes.

Note: For more information about managing passwords in CA SOI, see the *Implementation Guide*.

Connector Data Not Imported

Symptom:

CA SOI is not importing connector data.

Solution:

There are two possible reasons:

1. The connection to the SA Store database may have failed. Configure the database connection failure email notifications (see page 52). If there is a failure, the email provides the resolution.
2. A connector connection has failed. Configure the connector failure email notifications (see page 52). If there is a failure, the email provides the resolution.

Connector Not Online

Symptom:

I started my connector, but the connector status is not Online.

Solution:

Review the following points to determine why the connector is not Online after it is started:

- The connector could have trouble connecting to its domain manager, or it may not have published the data to the SA Manager yet.
- Use the status description of the connector, and, if necessary, the appropriate log files to determine whether there is an issue.
- Check the Status Description field for the connector in the CA SOI Administration UI. You can also enable DEBUG to see details of the connector status in its <*ConnectorName*>_HEARTBEAT_PUB.txt file.

  For example, if "Waiting for Connector Specific Initialization" is the last status in the <*ConnectorName*>_HEARTBEAT_PUB.txt file, there can be a problem with connecting to the domain manager. Make sure that the domain manager is accessible, and check the connection details that are provided for the domain manager in the connector configuration.
- Check the SAM-IntegrationServices_wrapper.log file for specific messages regarding the connector. This information can help you identify whether the connector is having issues connecting to the domain manager.
- Connector names have been added to messages in the ifw.log file to make it easier to trace individual connector processing. You can review these messages to get more specific information.

Note: For more information about troubleshooting connector shutdown behavior, see How to Troubleshoot Connector Shutdown Behavior (see page 99).

Connector Unable to Connect to the SSL-Enabled Domain Manager

Symptom:

A connector is unable to connect to the SSL-enabled domain manager.

Solution:

If SSL is enabled on the integrated domain manager, configure the connector to connect to the domain manager using SSL. You also must ensure that the CA SOI Dashboard can launch an SSL-enabled domain manager UI.

Follow these steps:

1. Open SOI_HOME\resources\Configurations\<*connector configuration file*> on the connector system.
2. Locate the LICURLS section, provide the appropriate HTTPS protocol and port values, and save the file.

   The file contains the correct information for connecting to the domain manager configured for SSL.
3. Verify that you can launch the domain manager UI from the connector system using the specified protocol and port information.
4. Import the security certificate for your integrated domain manager as follows:
   a. Obtain the installcert java file from a reliable location and download it to SOI_HOME\jre\bin on the connector system.

   b. Use the JDK installed with CA SOI on the connector system to compile the program from the command line as follows:
   `SOI_HOME\jre\bin\javac InstallCert.java`

   c. Run the compiled program using the following command:
   `java InstallCert <DomainServer>:<SSLport>`

   DomainServer

   Specifies the domain manager host name. This name must match the URL host entry that is specified in the connector configuration file. In many cases, the name is the short form of the host name and not the FQDN. If the short name is used, then the URL host entry must also be the short form.

   SSLport

   Specifies the SSL port.

   The program runs, and a prompt appears to save the certificate to a trusted keystore.

   d. Enter 1 to save the certificate to a key store file named jssecacerts, which gets created in the local directory.

   e. Copy the jssecacerts key file to SOI_HOME\jre\lib\security.
5. Restart the CA SAM Integration Services service.

   Note: Verify that the host name in the LICURLS section of the connector configuration file matches the host name that is used. Change the name if necessary, and save and close the file.

   The connector is configured to connect to the SSL-enabled domain manager.

No Connector Data in the Operations Console

Symptom:

My connector is ONLINE, but I do not see any corresponding data in the Operations Console.

Solution:

Because data is retrieved and sent through multiple checkpoints, it is necessary to trace it from the domain manager to connector to CA SOI. However, there are a few simple diagnostics that you can try before getting into the details:

- If you believe the connector published alerts, check the Alert Queues tab in the Operations Console. CIs do not have to be modeled into a service before their corresponding alerts populate the default alert queue.
- CIs that have not been modeled into a service, or imported as part of a service, do not appear in the Operations Console. From the Modeler, use the Browse By, Data Source option to see if there are any CIs that are imported from your connector.
- To determine if any data is associated with your connector in the database, use the CA SOI toolbox.
- If no data is associated with your connector in the database, it is necessary to trace the data (see page 42).

Anti-virus Programs Affecting the Connector Performance

Symptom:

My anti-virus programs are impacting the connector performance. How do I improve the performance?

Solution:

Anti-virus programs that perform real-time scans on open or updated files can affect the connector performance. For example, real-time scans could be occurring every time a connector log file is updated.

To eliminate this problem, you can exclude the following files in the SOI_HOME directory from the real-time virus scans:

- *.log
- *.xml
- *.xsd
- *.txt

- *.out
- *.conf
- *.tmp

How Do I Troubleshoot Connector Connection Problems?

Symptom:

I am having some connection problems with my connector (that the IFW manages). How can I troubleshoot this issue?

Solution:

To verify whether connectors (running under the IFW) are online and running in CA SOI, use the Connection Status button in the Operations Console. If the connector does not appear or shows as offline, do the following tasks to troubleshoot the problem:

- Check the install log file specific to your connector in the SOI_HOME\log directory for connection errors.
- Check the connector configuration file under SOI_HOME\resources\configurations and verify that it has the correct connection information. You can also access the content from the Administration UI.
- Ping the domain manager server from the computer where the connector is installed and verify that you can connect.
- Review the SAM-IntegrationServices_wrapper.log file (see page 101), heartbeat history for the connector (see page 101), connector message in the UI (see page 102), and email notification for the connector (see page 102).

How Do I Troubleshoot the Event Connector?

Symptom:

I am facing an issue with the Event connector. How do I troubleshoot the Event connector to resolve the issue?

Solution:

If you notice problems with the Event connector after installation, use the following points to troubleshoot the connector:

- Review the CA_Event_Integration_InstallLog.log file that is located in the root of the installation directory. This log primarily shows items such as installation errors related to file copies and configuration settings.
- Review the install.log file that is located in the EI_HOME\Logs directory. This log shows pre-installation or post-installation errors such as database creation failure and connector registration problems.
- Open the CA Event Integration administrative interface and verify that a connector displays in the Connectors tab for the Event connector system. If the connector does not display in the interface, registration with the CA Event Integration manager failed. For manually registering the connector with the agent, run the following command from EI_HOME\Core\bin on the connector system:

  ```
  register_agent EI_Manager_host 8083 connector_host 8083
  ```

- Verify that the samevent catalog was created and assigned to the connector. Check the catalog contents to verify the correct contents. Also check the sampc-dest.xml file to verify that the CA SOI connection settings are accurate.
- Ensure that you include the CIs created by the Event connector in services only if you want to see the alerts in the context of services.

How Do I Troubleshoot the Connector Policy?

Symptom:

I am facing some issues with my connector, and I want to troubleshoot the connector policy.

Solution:

The eitransform.log file contains information about all policy operations (such as parse, normalize, and format) included in your connector policy. This log file helps you find out whether the information is getting processed correctly, in case you encounter any issues. Enable this log file before you can start using it for troubleshooting problems with your connector policy. You can find the eitransform.log file at *SOI_HOME*\log after it is enabled.

Note: The size of the eitransform.log file grows quickly, so use caution when enabling it.

Follow these steps:

1. Locate and open the log4j.xml file available at *SOI_HOME*\resources.
2. Uncomment the following entry, and save and close the file:

   ```
   <!-- FOR EI TRANSFORMATION DETAIL -->
   <logger name="com.ca.eventplus.catalog" additivity="false">
   <level value="DEBUG" />
       <appender-ref ref="EITransform" />
   </logger>
   ```

   The eitransform.log file is now enabled.

3. Restart the CA SAM Integration Services service.

How to Troubleshoot Connector Shutdown Behavior

As a CA SOI administrator, you need immediate notification whenever any connector shuts down in your IT infrastructure so that you can take quick actions and can resolve the issue. CA SOI provides notifications and detailed logging whenever a connector shuts down. This improved and faster notification mechanism contains detailed information about the connector shutdown behavior, including an appropriate reason for the shutdown. The availability of the relevant information in the log messages helps you troubleshoot connectors, keep track of the connector status in your infrastructure, and take any prompt actions, if necessary. You can review the related log files to find more information about any anomaly that you encounter in the connector behavior. The easy identification of the problem that is associated with the connector also lets you manage your domain managers more efficiently.

The Integration Framework (IFW) as part of its heartbeat mechanism sends detailed description of the connector status to the SA Manager. The IFW sets and maintains a connector property *statusDesc* for this purpose. The statusDesc property includes information about the connector status and any error conditions that occur. The SA Manager reads and stores the property value to display it to the user in the product UI. The connector status information is also logged in the SAM-IntegrationServices_wrapper.log file and <*ConnectorName*>_HEARTBEAT_PUB.txt file.

The enhanced connector notification and logging mechanism, therefore, helps you as follows:

- Logs the appropriate reason (for example, Administration UI stop, connector failure, IFW shutdown) for the connector shutdown in the log file, SAM-IntegrationServices_wrapper.log. Review the log file to view the message; an example message that is included in this log file is as follows:

  ```
  2012/11/26 01:33:57 : abc-vm02.xy.com :
  CA:00056_service-discovery@abc-vm02.xy.com : OFFLINE - Connector was stopped
  from Administration UI. : Broadcasting HeartBeat Message
  ```

- Includes the shutdown message in the connector status notification as part of the *heartbeat* message. The heartbeat message is logged in the <*ConnectorName*>_HEARTBEAT_PUB.txt file. Review this file if you want to see the message included in the statusDesc property. An example message that is included in this file is as follows:

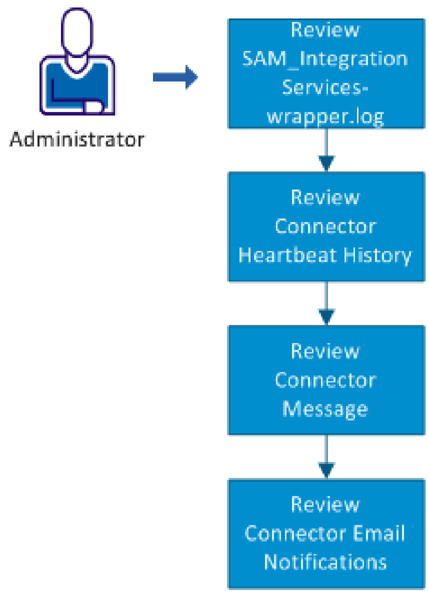
  ```
  statusDesc=Connector was stopped from Administration UI.
  ```

- Displays the reason for the connector shutdown in the Administration UI and Console.
- Sends an email notification to the CA SOI administrator about the connector shutdown.

For example, consider a scenario where a connector is stopped from the Administration UI. In this case, an appropriate message about the connector status is displayed at various locations. You can see the message in the product UI, SAM-IntegrationServices_wrapper.log file, <*ConnectorName*>_HEARTBEAT_PUB.txt file (if enabled), and in the email that is sent to the administrator (if enabled). By reading the message, you can quickly identify the reason for the connector shutdown and take appropriate measures.

Use this scenario to guide you through the process:

How to Troubleshoot Connector Shutdown Behavior


Administrator
Review SAM_Integration Services-wrapper.log
Review Connector Heartbeat History
Review Connector Message
Review Connector Email Notifications

1. Review the SAM-IntegrationServices_wrapper.log File (see page 101).
2. Review the Heartbeat History for the Connector (see page 101).
3. Review the Connector Message in the UI (see page 102).
4. Review the Email Notification for the Connector (see page 102).

Review the SAM-IntegrationServices_wrapper.log File

When a connector shuts down, CA SOI immediately logs the appropriate reason for the connector shutdown in the SAM-IntegrationServices_wrapper.log file. You can review and analyze the reason and perform the required steps to fix the issue.

Follow these steps:

1. Navigate to the *SOI_HOME*\jsw\logs folder.

   Note: *SOI_HOME* represents the location where CA SOI is installed; for example, C:\Program Files\CA\SOI.

2. Locate and open the SAM-IntegrationServices_wrapper.log file.

   The log file opens in a text editor.

3. Search for the connector status message.

   The following example shows a connector status message that is logged to this file:

   ```
   2012/11/26 01:33:57 : abc-vm02.xy.com :
   CA:00056_service-discovery@abc-vm02.xy.com : OFFLINE - Connector was stopped
   from Administration UI. : Broadcasting HeartBeat Message
   ```

Review the reason for the shutdown.

Review the Heartbeat History for the Connector

CA SOI includes the shutdown message in the connector status notification as part of the heartbeat message that is periodically sent to the SA Manager. By reviewing the heartbeat history for the connector, you can determine the trend in the connector behavior.

The statusDesc property value in the connector debugData logs describes the status of the connector for which the heartbeat is sent. Enable the debugData logging for the connector (enabled in the log4j.xml file). After you enable the debug logging, a file <*ConnectorName*>_HEARTBEAT_PUB.txt is created and displays the heartbeat history for the connector. The connector writes any published heartbeat messages into this text file.

Follow these steps:

1. Navigate to the *SOI_HOME*\resources folder.

2. Locate and open the log4j.xml file in a text editor.

   The file opens in a text editor.

3. Modify the *com.ca.sam.ifw* level to DEBUG.

   The debugData logging is enabled for the connector.

4. Verify that the <ConnectorName>_HEARTBEAT_PUB.txt file is created under the *SOI_HOME*\log\debugData folder when the connector writes any published heartbeat message.
5. Open the file in a text editor and start reviewing the heartbeat messages in the file.

   An example of how the statusDesc property is displayed in the file is as follows:

statusDesc=Connector was stopped from Administration UI.

Review the Connector Message in the UI

The SA Manager parses and stores the status description property value to display it to the user in the Administration UI and Console. The SA Manager receives this value as part of the heartbeat message that the IFW periodically sends to the SA Manager. When the connector goes offline for any reason, a relevant message is displayed in the Administration UI and Console as appropriate. This message includes detailed connector status and reasons for the shutdown (if any).

The Dashboard Administration tab provides a field named Status Description that provides detailed connector status information. This information is identical to the most recent entry in the Operation Console Connection Status dialog Message field.

To fix the issue, review and analyze the information that is provided in the message and perform relevant tasks.

Review the Email Notification for the Connector

When the connector goes offline, CA SOI notifies the specified administrator by sending an email. The email notification includes information about the failure.

To fix the issue, review and analyze the information that is provided in the email and perform relevant tasks.

An example of an email notification that is sent to the administrator when you stop any connector from the Administration UI is as follows:

```
SOI Manager - Connector 'build.abc.com:CA:09998_build.abc.com@build.abc.com' on
SOI Manager build.abc.com is off-line and has not been restarted. The reported
reason is 'Connector was stopped from Administration UI'
```

Note: If the administrator email is not configured in the Administration UI, specify the appropriate email ID to receive failure notifications by email. For more information, see Configure the CA SOI Administrator Email for Error Notification (see page 103).

Configure the CA SOI Administrator Email for Error Notification

You can configure the CA SOI administrator email in the Administration UI so that CA SOI can notify the administrator by email about failures.

Follow these steps:

1. Click the Administration tab.
2. Click the plus sign (+) next to CA SOI Insight Manager Configuration.

   Click the plus sign (+) next to the server you want to configure.
3. Click Error Notification Configuration.
4. Enter the full email address for the administrator in the Administrator Email section.
5. For the Connector Failure Notification Settings section, perform the following actions:
   1. Select Yes from the drop-down to turn on email notifications.
   2. Enter the number of minutes until CA SOI sends the email notification.
6. Click Save.

Sample Connector Changes Are Not Reflected in CA SOI

Symptom:

I made changes to the Sample connector sample data files; however, I do not see those changes in CA SOI.

Solution:

If you make changes to the Sample connector sample data files or connector policy and these changes are not reflected in the Sample connector data that CA SOI displays, check the location of the files you manipulated.

Sample data and policy files for the Sample connector exist in the following places:

SOI_HOME\resources

Contains data and policy files that the Sample connector uses during runtime.

SOI_HOME\resources\SampleConnector\data

Contains sample data files.

SOI_HOME\resources\Core\Catalogpolicy

Contains connector policy files.

SOI_HOME\SampleConnector

Contains the code that implements the Sample connector and the framework for building a custom connector.

If you want to make changes to the sample data or policy files and see the effect on a running Sample connector, make the changes in the SOI_HOME\resources\SampleConnector and SOI_HOME\resources\Core\Catalogpolicy directories and restart the CA SAM Integration Services service. Changing the files in the SOI_HOME\SampleConnector directory has no effect on a running Sample connector.

Unable to View CA Catalyst r3.2 Connectors in CA SOI r3.x

Symptom:

I cannot view my CA Catalyst r3.2 connectors in CA SOI r3.x.

Solution:

The IFW Proxy provides access to data from CA Catalyst r3.2 connectors to CA SOI. For more information about the IFW Proxy, see the *Connector Guide*.

Verify the Universal Connector Web Service

Use your web browser to verify whether the Universal connector web service on the CA SOI computer responds to queries. You can do this by verifying that the Web Services Description Language (WSDL) file content is displayed in an XML-like syntax and a list of available services for GenericConnectorService is displayed in a user-readable format.

- For WSDL, enter the URL *http://<SAManager_server>:7090/axis2/services/GenericConnectorService?wsdl* in your browser window. The web browser displays the WSDL file content in the appropriate XML format if the web service is responding correctly.
- For the list of available services, enter the URL *http://<SAManager_server>:7090/axis2/services/listServices* in your web browser window. The web browser displays the list of provided services for GenericConnectorService in a user-readable format if the web service is responding correctly.

Verify the Universal Connector Files

You can verify whether the appropriate Universal connector files are correctly installed. After the installation, you can search for a few files on the computer as follows:

- To verify the Universal connector files on the CA SOI computer where the Universal connector server is located, search for the following files:
  - SOI_Home\lib\ca-sam-connector-universal-server.jar
  - SOI_Home\lib\generic\*.jar
  - SOI_Home\tomcat\webapps\axis2 folder
- To verify the Universal connector files on the Universal connector client computer, search for the following files:
  - SOI_Home\lib\ca-sam-connector-universal-client.jar
  - SOI_Home\GCEventAddCmd.bat
  - SOI_Home*.xml sample files

Dashboard Troubleshooting

The troubleshooting topics in this section relate to the CA SOI Dashboard.

Administration Tab or Dashboard Links Not Working with Firefox

Symptom:

I am experiencing either or both of the following errors when accessing the Dashboard with Mozilla Firefox:

- I click the Administration tab, but the interface does not open.
- I click any of the Dashboard links (Google Earth, Console, and so on), but nothing happens.

Solution:

This problem can result from a conflict between some versions of Firefox (before v17.x and after v18.x) and the Java Deployment Toolkit plugin.

Follow these steps:

1. If you are running Firefox, verify that you are using a version later than 12 and upgrade to a later version if required.
2. If you are unable to upgrade to a later version of Firefox, disable the Java Deployment Toolkit plugin in Firefox. This plugin checks for Java updates.

Administration Tab Values Not Saving

Symptom:

When I update values on the Dashboard Administration tab, CA SOI does not save the values.

Solution:

This issue is related to the browser security. Add the UI server to your web browser trusted sites and allow cookies from the domain.

Follow these steps:

Note: The following example uses Internet Explorer. For a list of supporter browsers, see the *Release Notes*.

1. Add the UI server to your Internet Explorer web browser Trusted Sites:
   a. Select Tools, Internet Options.
   b. Click the Security tab then click Sites.
   c. Click Advanced.
   d. Enter the fully qualified domain name of the UI server and click Add.
2. Allow cookies from the UI server:
   a. Select Tools, Internet Options.
   b. Click the Security tab then click Sites.
   c. Enter the domain name (for example, mydomain.com) of the UI server and click Allow.

Alerts Not Created

Symptom:

CA SOI is not creating alerts.

Solution:

1. The connection to the SA Store database may have failed. Configure the database connection failure email notifications (see page 52). If there is a failure, the email provides the resolution.
2. See Alert Flow in CA SOI and Log File Outputs (see page 46) to trace alert problems.

CIs Not Created

Symptom:

CA SOI is not creating CIs.

Solution:

1. The connection to the SA Store database may have failed. Configure the database connection failure email notifications (see page 52). If there is a failure, the email provides the failure details and a link to the resolution.
2. See CI flow in CA SOI and Log File Outputs (see page 42) to trace CI problems.

Failure Notification Emails Not Sending

Symptom:

I have activated the failure notifications, but the emails do not send.

Solution:

1. If you are sending the email to multiple addresses, verify that you are using commas (,) to separate the emails; semicolons (;) do not work.
2. Test the email server by manually sending an alert email:
    a. Log in to the Operations Console.
    b. Select an alert and click the envelope icon.
    c. Complete the email dialog and send the email.
3. Verify the correct mailhost is defined in the following location:

    \Windows\System32\drivers\etc\hosts file
4. Restart the SA Manager service.

Google Earth Does Not Display New or Updated Locations on the Map

Symptom:

I have set or updated a service location on the Operations Console, but Google Earth does not update the location on the map.

Solution:

There is a known issue with Google Earth 7.0. If you edit or modify the service location while Google Earth is open, the location shows immediately on the Google Earth Places list, but can take 20 to 30 minutes to update on the map. As a workaround, restart Google Earth and the updated locations appear immediately on the map.

Event Management Troubleshooting

The troubleshooting topics in this section relate to Event Management.

Event Management Connection Problems

Symptom:

The Event Management components are failing or unable to integrate with certain data sources.

Solution:

Perform the following actions:

- Verify that the CA SAM Event Management Service is running on the SA Manager and connector systems.
- Verify that each connector appears as Online in the Operations Console and the Administration UI.
- To see an updated list of available connectors, refresh the Events tab.

Event Search Returns no Results or Unexpected Results

Symptom:

An event search returns no results or unexpected results.

Solution:

Verify the following items:

- Verify that you are using the correct properties and values that are listed in the Event Properties and Event Information section in the *Administration Guide*.
- If you are using optional properties in search patterns, verify that the appropriate data sources produce that property.
- Verify that the pattern syntax adheres to the conventions in the Event Search Syntax Guidelines and Best Practices section in the *Administration Guide*.
- Try using the 'ANY event occurs' criterion first, because it does not consider time intervals. Once you have established that events exist that match the patterns, try a time-based pattern detection.
- If you receive an error message before the results display that you need help interpreting, see the section on error messages (see page 111).

Expected Alerts Not Appearing on Operations Console After Processing

Symptom:

Alerts are not appearing on the Operations Console after Event Management processing. For example, events do not appear as alerts.

Solution:

Perform the following actions:

- Verify your alert filter settings at the IFW level. The IFW or specific connectors may be preventing alerts that do not affect services from appearing.

  Note: For more information about configuring IFW and connector filter settings, see the *Connector Guide*.

- To verify that you are not filtering out alerts that you want to see, view the applied alert filters at the Operations Console level.

  Note: For more information about alert filters, see the Create an Alert Filter section in the *Administration Guide*.

- To verify that you are not prevented from seeing alerts that are appearing in specific queues, view the defined alert queues and their access privileges.
- All alerts must be associated with a valid CI.

Event Policies Not Producing Expected Actions

Symptom:

Deployed event policies are not producing the expected actions. For example, enrichments are not occurring.

Solution:

Perform the following actions:

- See the section about error messages (see page 111) for help interpreting any errors that appear while creating policy.
- Verify that a file for the policy exists in the SOI_HOME\resources\EventManagement\Policies directory. Print this file for a record of the raw policy syntax.

- Enable detailed transformation policy (see page 98) logging for a more granular view of connector and event policy operations. The SOI_HOME\log\eitransform.log file includes operations that even policies add. This log file helps you find out whether the information is processed correctly. Enable detailed transformation logging in the eitransform.log file before you can start using it for troubleshooting your event policy. You can track individual operations that occur based on your event policies. For example, you can see whether trap properties are being normalized properly.
- If you changed the enrichment connection information (for example, edited script parameters), restart the CA SAM Integration Services service.
- Policies that you create through the user interface do not support aspects of certain actions, such as combining include and exclude filters. If the user interface does not provide the functionality that you require, consider refining your policy manually.

How Do I Control the Event Management Data Flow to the Operations Console?

Symptom:

I want to control the Event Management data flow to the Operations Console so that I can manage my events more efficiently. How can I do that?

Solution:

To decide how you want to control the Event Management data flow to the Operations Console, configure the eventManagerClientConfig.xml configuration file.

Follow these steps:

1. Open the SOI_HOME\tomcat\lib folder.
2. Locate and right-click the eventManagerClientConfig.xml file, and select Open With, Notepad from the context menu.
3. Configure the following parameters, and save and close the file:

   timeoutValues

   Specifies the amount of time in seconds that the event service waits for a response to a query request. Each type of request can have its own value. You can set the timeout values for the following actions:

   - DeployPolicy
   - DeployScript
   - GetConnectorInfo
   - GetDeployedPolicy
   - GetDeployedScript
   - GetEvents

synchInterval

Specifies the polling interval in seconds for determining the available event services. The list of data sources available in the Event Policy dialog (Tools, Event Policies) in the Operations Console reflects the current state of this polled information. Any changes to the status of data sources can take up to the interval time (specified for this parameter) to update in the Operations Console.

Default: 45

4. Restart the CA SAM Application Server service.

Searches Taking Too Long

Symptom:

The event searches are taking too long, or the data source information is incorrect.

Solution:

Edit the timeout values in the eventManagerClientConfig.xml (see page 110) file.

Error Messages on an Event Result Error Dialog

Symptom:

I received an error message on an Event Result Error dialog when I ran an event search. How do I interpret the error message?

Solution:

The following messages can appear on an Event Result Error dialog when you run an event search and click a result button that has turned yellow or red:

***Connector name*: No events matched**

Indicates that the search returned no matches for a connector that you included in the scope. After you close the dialog, events may appear for other connectors included in the scope. This error does not indicate a problem with the search itself or the returned results. The error is only a notification that at least one scoped source returned no results. In response to this message, you can either refine your search if you want to return events from that source, or do nothing and simply work with the returned results if the search is accurately scoped and defined.

***Connector name*: Warning:droolsconvert_failed**

Indicates that some portion of the search syntax cannot be converted to the Drools language. The actual Drools conversion takes place when you save or deploy an event policy. Therefore, this warning does not affect the accuracy of a simple event search, but creating an event policy based on the search will fail. Common reasons for Drools conversion failure include the use of unsupported functions or inappropriate use of operators (for example, a greater than or less than operator with non-numeric values). For specific information about the error, see the EventMgmt.log file at SOI_HOME\log.

For more information about constructing valid searches, see Event Search Synta*x* Guidelines and Best Practices.

***Connector name:* Connector is not available for request**

Indicates that Event Management could not access the connector to query its events. Check the status of each connector if this error occurs.

***Connector name:* Request timed out. Event Service did not respond within 30 seconds.**

Indicates that the search did not complete due to an unresponsive Event Service. Check the status of the CA SAM Event Management service if this error occurs.

Large event set matched. Reduce the scope.

Indicates that the search returned more than 25,000 events for a single data source, which is the upper limit for search results per connector. You must reduce the scope, either through time range or data sources, to return an acceptable number of events.

An Internal error occurred. Please check server logs

Indicates that an unspecified error occurred that prevented the search from completing. To investigate the source of the error, see the EventMgmt.log file at SOI_HOME\log.

Policy file not found

Indicates that a saved or deployed policy that you selected on the Events tab is not available in its expected location, and its pattern does not display in the Event Search tab. Verify that the policy file exists on the SA Manager at SOI_HOME\resources\EventManagement\Policies.

The following messages may appear when you click Create Policy or Map Events on the Event Search tab:

Note: Some of these error messages also appear when you click the result button.

Map Events needs search results

Indicates that no current search results exist for the entered raw event search pattern. Completing a raw event search is required before creating a normalization action based on that search, so that you can use the results to access the raw event properties for mapping. The message gives you the option to continue, but no raw event properties are available to map on the Normalize Event page.

Error: Unable to Resolve: property='value

Indicates that the event search is invalid due to a missing quotation mark on either side of the property value. Add the missing quotation mark and rerun the search.

Error: OR operands NOT supported in policy deployment for Raw Events

Indicates that the raw event search uses an OR operand. The search returns valid results, but event policies that are based on the raw event searches do not support the use of this operand.

Error: Operator: NOT supported in policy deployments for Raw Events

Indicates that the raw event search uses an operator that is not supported in event policies that are based on the raw event searches. Only the '=' operator is supported in this situation.

Error: Operator: NOT supported in policy deployments for Normal Events

Indicates that the normalized event search uses an operator that is not supported in event policies that are based on the raw event searches. Only the '=' and ‘!=’ operators are supported in this situation.

Error: ‘not’ syntax incorrect. Not supported in policy deployments pattern

Indicates that the event search uses unsupported syntax. For details, see the section Event Search Syntax Guidelines and Best Practices in the *Event and Alert Management Best Practices Guide*.

Error: ‘contains’ / ’starts-with’ / ’ends-with’ is NOT supported in policy deployments pattern

Indicates that the event search uses a function that is not supported in event policies.

The following messages can appear on the Create Event Policy dialog when you try to deploy or save an event policy:

Search errors

Indicates that the search errors previously listed can appear in the Event Log table that displays the current search results for use in previewing how a create event or enrich event action affects an event.

UNKNOWN_ERROR - [QueryParms.ConvertToEIPolicy: Drools conversion failed, see log files]

Indicates that some portion of the search syntax cannot be converted to the Drools language. This message appears after you click Finish on the Select Data Sources page. The Drools conversion takes place when you save or deploy an event policy, and the operation is prevented if Drools conversion fails. Common reasons for Drools conversion failure include the use of unsupported functions or inappropriate use of operators (for example, a greater than or less than operator with non-numeric values). For specific information about the error, see the SOI_HOME\tomcat\logs\soimgr.log file.

For more information about constructing valid searches, see the Event Search Syntax Guidelines and Best Practices section in the *Administration Guide*.

One or more Data Sources are currently disabled!

Indicates that one or more connectors are currently unreachable. This message appears on the Select Data Sources page. You can complete the policy creation if all of the data sources that you need are available.

Various other warnings appear at the bottom of the Create Event Policy dialog when input is required before you can progress to the next page.

How to Search Archived Event Store Files?

Symptom:

I want to search archived the Event Store files for event searches that are not time-scoped.

Solution:

To search archived the Event Store files, configure the EventManager-wrapper.conf file.

Follow these steps:

1. Open the SOI_HOME\jsw\conf\EventManager-wrapper.conf file.
2. Add the following Java define as necessary or change its default value in the Java Additional Parameters section, and save and close the file:

EQUERY_UNZIP_ARCHIVE=

Determines whether to unzip and search the archived Event Store files for event searches that are not time-scoped. Enter 1 to search archived files. The value 0 implies that you do not want to search archived files.

Default: 0

Preface the parameter with the correct additional Java parameter syntax and the appropriate sequential number, as shown in the following example:

```
wrapper.java.additional.2=-DEQUERY_UNZIP_ARCHIVE=1
```

3. Restart the CA SAM Event Management service.

   Subsequent event searches use the configured settings.

Not Enough Event Groups in Search Results

Symptom:

I want to increase the number of event groups in search results so that more groups are returned in results.

Solution:

To create the maximum number of event groups in search results, configure the EventManager-wrapper.conf file.

Follow these steps:

1. Open the SOI_HOME\jsw\conf\EventManager-wrapper.conf file.
2. Add the following Java define as necessary or change its default value in the Java Additional Parameters section, and save and close the file:

   ESTORE_MAX_QGROUP=

   Determines the maximum number of groups to return in search results.

   Default: 10

   Preface the parameter with the correct additional Java parameter syntax and the appropriate sequential number, as shown in the following example:

   ```
   wrapper.java.additional.3=-DESTORE_MAX_QGROUP=10
   ```

3. Restart the CA SAM Event Management service.

   Subsequent event searches use the configured settings.

Event Processing Performance Due to Mid-Tier Connector

Symptom:

I am experiencing some event processing performance issues due to the Mid-Tier connector. The Mid-Tier connector is not required in my infrastructure for event processing. How can I disable it?

Solution:

You can disable the Mid-Tier connector if the holistic action processing layer that it provides is not necessary for your Event Management implementation. Bypassing the Mid-Tier connector if you are not using it for event policies improves the event processing performance. The setMTCstate utility disables the connector and reroutes events so that they proceed directly to the SA Manager from connectors.

Run this utility on the SA Manager system. The utility assumes the default Mid-Tier connector configuration, with one Mid-Tier connector that is installed on the SA Manager.

Follow these steps:

1. Shut down the Mid-Tier connector using the CA SOI Administration UI.
2. Navigate to SOI_HOME\Tools on the SA Manager and run the following command:

   ```
   setMTCstate Disabled
   ```

   The Mid-Tier connector is disabled.

   Note: You can also enable the Mid-Tier connector if you have previously disabled it by substituting the term Enabled for Disabled.
3. Restart the CA SAM Application Server service.

   The change is applied and the connector is disabled.

Help Desk Integrations Troubleshooting

The troubleshooting topics in this section relate to the CA SOI integration with help desk products.

CA Service Desk Integration Troubleshooting

If you cannot connect to CA Service Desk or create CA Service Desk tickets in CA SOI, do the following to troubleshoot CA Service Desk connection problems:

- Verify that the connection settings are correct on the Help Desk Configuration page of the Administration UI. Click Test to test the connection.
- If CA Service Desk is configured for SSL, verify that you selected the SSL check box. The integration does not work if this check box is not synchronized with the CA Service Desk SSL configuration.

  For more information, see Export CA Service Desk SSL Certificate.
- Try to access the following CA Service Desk URL independent of CA SOI:

  ```
  http://ServiceDeskServer:ServiceDeskPort/axis/services/
  USD_R11_WebService?wsdl
  ```

  Note: The default CA Service Desk port is 8080.

  If you cannot reach this URL, do the following:

  - Verify that the Service Desk Web Services component is installed on the CA Service Desk system. This component must be installed for the integration to work.
  - See the CA Service Desk documentation.
  - If you are using CA Service Desk r12.1 that has been upgraded from a previous release, clear the CA Service Desk browser cache.

CA Service Desk Ticket Not Created by Escalation Policy Action

Symptom:

I have configured an escalation policy action to create a CA Service Desk help desk ticket, but CA SOI does not create the ticket.

Solution:

Follow these steps:

1. Try to create the ticket manually. If the ticket fails, note the error message that is returned. For more information about creating a ticket manually for CA Service Desk, see the CA SOI *Administration Guide*.
2. Review the CA SOI escalation policy action to verify that any CA Service Desk specific values such as the template, requested area, and assignee are valid values in CA Service Desk.
3. Verify that there is a Description property with a value set. Certain versions of CA Service Desk does not work without a Description property.

Cannot Create a BMC Remedy or HP Service Manager Ticket in CA SOI

Symptom:

I cannot create a BMC Remedy or HP Service Manager Ticket in CA SOI.

Solution:

Follow these steps:

1. Verify the connection to CA Process Automation in the CA SOI Administration tab Help Desk Configuration screen. For more information about configuring CA SOI, see the *Administration Guide*.
2. Verify the connection to BMC Remedy or HP Service Manager using the CA Process Automation TestRemedyServerConnection (BMC Remedy) Form or the TestHPSMServerConnection (HP Server Manager) Form. For more information about testing a connection, see the *Implementation Guide*.
3. Create a test ticket in BMC Remedy or HP Service Manager using the CreateRemedyTicket (BMC Remedy) Form or the CreateTestTicket (HP Service Manager) Form. For more information about creating a test ticket, see the *Implementation Guide*.

HP Service Manager Integration Troubleshooting

Use the following information to troubleshoot issues with the HP Service Manager integration:

Triggers are not initiated when a user in HP Service Manager edits an incident that the integration created.

- Verify that the “us.launch.external.NEW” application is installed on the HP Service Manager server. If the application is not installed, download it from HP Support.
- The launch in context URL that opens when you click a Ticket ID in CA SOI does not show the incident details in HP Service Manager.
- Verify that the following parameters in the web.xml file of the HPSM Web Client have the following values:

Property Name	Value
querySecurity	false
useservertabs	true
essuser	false

Ticket Creation, Closure, or Update is Failing

Symptom:

Any or all of the following help desk ticket problems occur:

- I created a ticket in CA SOI, but the ticket does not appear in the help desk product.
- I cleared an alert in CA SOI, but the ticket does not close in the help desk product.
- I updated the alert in CA SOI, but the ticket does not update in the help desk product.

Solution:

Use the following process to resolve the problem:

1. Review the escalation policies and actions. Verify that the policies are valid.
2. There could be a connection problem to the CA Process Automation server or the help desk server. The failure results in escalation actions for help desks failing or the synchronization of certain CA SOI properties with the help desk ticket failing. Configure email notifications for third-party server failures (see page 52) to determine if this is the cause. The email provides failure information.
3. In CA Service Desk, look in the Action History table for an error message that is related to the ticket.
4. In CA Process Automation, look for workflow error messages for BMC Remedy or HP Service Manager tickets.

Ticket Status Changed when Connector Shut Down or Removed

Symptom:

When I shut down or remove a connector, CA SOI changes the status of tickets to Closed or another status.

Solution:

In the Help Desk Configuration dialog (Operations Console menu: Tools, Help Desk Configuration), you set the option "Auto change trouble ticket status when alert is cleared." When you shut down or remove the connector, CA SOI changes to the status you specified for all cleared alerts or Closed, by default. You cannot undo this operation.

Integration Framework Troubleshooting

The troubleshooting topics in this section relate to the IFW.

Java Heap Space Out Of Memory Error

Symptom:

When I try to import a large number of CIs from a domain manager, I receive the Java heap space OutOfMemory error.

Solution:

If there are a large number of CIs, relationships, and services to be imported from a domain manager, the IFW may run out of allocated JVM heap space and stop responding. This error appears as a "java.lang.OutOfMemoryError:Java heap space" exception in the SOI_HOME\jsw\logs\SAM-IntegrationServices_wrapper.log file. You may need to increase the IFW JVM heap space if this situation occurs frequently to process all imported CIs and relationships.

Do any of the following tasks to manage the IFW JVM heap space:

- Increase the JVM heap size in the IFW (default is 1 GB) as follows:
  - Stop the CA SAM Integration Services service.
  - Increase the wrapper.java.maxmemory value (in MB) in the SOI_HOME\jsw\conf\SAM-IntegrationServices.conf file.
  - Start the CA SAM Integration Services service.
- Turn off the getRelationshipsAtStartup control for connectors with a large number of CIs and relationships. This operation prevents rediscovery of all relationships every time the connector starts. Importing services still imports all relationships with this control turned off.

Mobile Dashboard Troubleshooting

The troubleshooting topics in this section relate to the CA SOI Mobile Dashboard.

Service Names do not Appear on the Mobile Dashboard

Symptom:

When I access the Mobile Dashboard, the service names are empty.

Solution:

Service names on the Mobile Dashboard are obtained from the USM Properties that are named Service Name and Label.

It is possible that the USM properties were not created properly.

Follow these steps:

1. Stop the CA SAM Application Server service.
2. Navigate to the following folder:

   SOI_HOME\tomcat\registry\topology\physical\node0\sor
3. View the following files and verify it matches the server name with the output of %COMPUTERNAME% case sensitive.
   - restserver.xml
   - sorapp.xml
   - ssaserver.xml

   Example:

   ```
   <tns:brokerURL>tcp://<Computername>:61616</tns:brokerURL>
   <Computername> has to be the exact content of %COMPUTERNAME%
   ```
4. Open a cmd window, navigate to the SOI_HOME\tomcat\registry folder and run the command "registryloader".

   Note: Ignore any warning messages about log4j settings.
5. Perform one of the following actions:
   - For new created Services verify that the USM Properties "Service Name" and "Label" are correctly populated.
   - For existing Services run the Primerutility script in <SOI_HOME>\Tools\Priming Utility\ which creates the missing reconciled sheets.

Operations Console Troubleshooting

The troubleshooting topics in this section relate to the CA SOI Operation Console.

Access - Proxy Server Prompt Opens When Accessing the Operations Console

Symptom:

Every time I open the Operations Console, I must enter credentials in a proxy server prompt.

Solution:

You must configure your Java settings to use your browser settings or establish a direct connection when starting Java applications.

Follow these steps:

1. Launch the Java Control Panel.
2. Click Network Settings.
3. Select 'Use browser settings' or 'Direct connection', and click OK.
4. Click OK on the Java Control Panel.

Access - Unable to Start the Operations Console

Symptom:

When I try to open the Operations Console, the message "Unable to Launch Application" appears.

Solution:

Verify that you are using a Java version of 1.6.0_24 or above; if not, upgrade to a supported version. If the automatic installation does not work, manually download and install the latest JRE from the Java website and try to launch the Operations Console again.

If you are using a supported Java version, try clearing the JNLP cache.

Follow these steps:

1. Launch the Java Control Panel.
2. Click the View button in the Temporary Internet Files section.
3. Right-click the extra CA SOI applications in the list, and select Delete.

Alerts - How Do I Find an Alert?

Symptom:

I want to track the flow of alerts in CA SOI to pinpoint the error. How can I trace an alert in CA SOI?

Solution:

Review the Alert Flow in CA SOI and Log File Outputs (see page 46) section in the guide. This section provides the complete flow of an alert. You can review the stages involved in the flow and the corresponding log file outputs to identify, analyze, and fix the error.

CIs - Domain Manager Administrative CI States not Reflected in CA SOI

Symptom:

I do not see the administrative CI state for my domain manager in CA SOI.

Solution:

Some domain managers are capable of setting administrative CI states (for example, CA NSM managed objects can be set to different states such as maintenance, unmanaged, and unknown). The states that are set in domain managers are not reflected in CA SOI. The corresponding CI displays a Normal status in CA SOI.

CIs - Duplicates Appear on the Operations Console

Symptom:

I see that duplicate CIs are appearing on the Operations Console.

Solution:

If duplicate CIs appear on the Operations Console that should have been correlated as one CI, check the DNS resolution settings in the source domain managers.

CIs - How Do I Find a CI?

Symptom:

I want to track the flow of CIs in CA SOI to locate the error. How can I trace a CI in CA SOI?

Solution:

Review the CI Flow in CA SOI and Log File Outputs (see page 42) section in the guide. This section provides the complete flow of a CI. You can review the stages involved in the flow and the corresponding log file outputs to identify, analyze, and fix the error.

CIs - Missing from CA SOI

Symptom:

I do not see CIs in CA SOI.

Solution:

If you do not see expected CIs in the CA SOI Operations Console or the staging area of the Service Modeler, they may have been rejected by a USM validation failure. The SA Manager validates CIs against the USM schema, and any CI that does not pass this validation is rejected and filtered out. A CI may fail USM validation for any of the following reasons:

- An error in connector policy that improperly converts the domain manager information to USM
- No data in a field that is required by USM
- The domain manager presents data in a way that cannot be processed by its connector policy

Check the SOI_HOME\log\ssa.log file to see if USM schema validation failures have occurred.

CIs - Property Values are Incorrect

Symptom:

I notice that some of the CI property values are incorrect. How do I correct them?

Solution:

If you notice that CI property values are incorrect (such as IP address, DNS name, and DeviceID), ensure that you adhere to the following best practices for DNS resolution and fixing incorrect values:

- If your environment uses DHCP, you must have DNS resolution enabled for all connectors.
- The IP address, SysName, and DNS name (when used) must be correct for managed objects in the domain manager. If necessary, rerun the discovery on the domain manager to correct these properties.
- If the IP address is incorrect in the domain manager, do not turn off DNS resolution on the connector. This approach makes the problem more severe.

Escalation Actions - CA Process Automation Forms Not Available

Symptom:

I am trying to create an escalation policy using the Execute Automated Process action type, but no CA Process Automation forms are available.

Solution:

CA SOI may have lost the connection to the CA Process Automation server.

Follow these steps:

1. Enable server connection error notifications on the Dashboard Administration tab.
2. Test the CA Process Automation server.
3. Restart the SOI Manager service.

Escalation Actions - Email Actions Not Sending

Symptom:

I have created an escalation policy or manually used Take Action to send an email, but CA SOI does not send the email.

Solution:

You may have entered multiple email addresses incorrectly or CA SOI may have lost the connection to the email server.

Follow these steps:

1. If you are sending the email to multiple addresses, verify that you are using commas (,) to separate the emails; semicolons (;) do not work.
2. Test the email server by manually sending an alert email:
   a. Log in to the Operations Console.
   b. Select an alert and click the envelope icon.
   c. Complete the email dialog and send the email.
3. Verify the correct mailhost is defined in the following location:

   \Windows\System32\drivers\etc\hosts file
4. Restart the SA Manager service.

Escalation Actions - Tickets Not Created

Symptom:

I have created an escalation policy to create a help desk ticket, but CA SOI does not create the ticket.

Solution:

CA SOI may have lost the connection to the help desk server.

Follow these steps:

1. Enable server connection error notifications on the Dashboard Administration tab.
2. Test the help desk server.
3. Restart the SA Manager service.

Escalation Actions - Resolve Escalation Action Failures

Symptom:

I received an email notification that CA SOI has stopped an escalation policy action because the action continues to fail.

Solution:

CA SOI provides an error notification that automatically retries failed actions for a specified time period and then disables the action.

The following procedures describe how to resolve an action failure that is based on the action type.

Clear Alert

Follow these steps:

1. Try to clear the Alert manually. Right-click the alert and select Clear Alert.
2. Check the Clear Alerts flag on the Global Settings page, which is available on the Dashboard Administration tab.
3. Turn on debug tracing on the SA Manager and view the debug information:
    a. Access the SA Manager Debug page.
    b. Click Web Server Debug Page (Runtime).

   c. Locate the Alarm Data Model module and change the Desired State to ON and click Apply.

   d. Check for errors in the soimgr-debug.log file (see page 20).

4. Enable the action once you resolve the error.

Create Announcement

Follow these steps:

1. Verify that all of the properties that are set for the Announcement are valid.
2. Verify that the help desk system is reachable and that the associated services are running.

Create Ticket

Follow these steps:

1. Verify that the Description ticket property is set in the action.
2. Verify that all properties set in the help desk system are valid.

Execute Automated Process in CA Process Automation

Follow these steps:

1. Review the failed process or form in the Default Process Watch in CA Process Automation.
2. Verify that the CA Process Automation server is reachable and that the CA Process Automation service is running.

Execute Command

Follow these steps:

1. Verify that the executable is in the system path.
2. Verify that the executable is functioning outside of CA SOI.

Send Email

Follow these steps:

1. Verify that the email server is configured. See email configuration documentation.
2. Ensure that a comma is used as a separator when using multiple email addresses.

Service Discovery - Default Significance does not Match CI Significance

Symptom:

I modified the default significance for a CI type (such as a Router). When I create dynamic relationships using Service Discovery, the significance is not reflected in the CIs.

Solution:

When you add CIs to a service in the Modeler, the default significance setting is evaluated dynamically on the UI Server. For the SA Manager to acquire these changes, restart the SA Manager service. The default significance is then assigned to new relationships that come in from Service Discovery or another connector.

Service Models - Resolve Looping Problems

Symptom:

CA SOI sent me an email notification that a looping problem can exist.

Solution:

You configured failure email notifications previously.

Perform the following actions to identify and resolve loops that CA SOI detects:

- A parent service is nested as a sub service of a child service.
  - Do not include the same service within its own service hierarchy.
  - To correct this type of loop, remove the child instance or parent service instance.
- Multiple linked bound relationships:
  - Do not attach bound relationships to other bound relationships.
  - To correct this type of loop, remove or replace one or more of the bound relationships with another relationship type.

SLA Recurrence Not Triggering

Symptom:

I have set an SLA to recur starting today, but it does not trigger.

Solution:

When you set the Recurrence date, it must be at least one day later than the Start Date. If the Start Date is Jan 1, 2013 and the Recurrence date is Jan 1, the first recurrence is Jan 1, 2014. However, if you set the Recurrence Date to Jan 2, the first recurrence happens on Jan 2, 2013.

SA Manager and UI Server Troubleshooting

The troubleshooting topics in this section relate to the SA Manager and UI servers and their services.

Disk Full

Symptom:

The disk where I installed CA SOI is full.

Solution:

You can use a command to shrink the Microsoft SQL transaction log file to free some space. However, your database must be configured with the recovery model Simple. If the recovery model is Full, the shrink command does not work.

Note: For more information, see the MSDN document http://support.microsoft.com/kb/907511.

Follow these steps:

1. Perform a full database backup using the following command:

```
BACKUP DATABASE [SAMStore] TO DISK = N'C:\Program Files\Microsoft SQL
Server\MSSQL.1\MSSQL\Backup\SAMStore.bak' WITH NOFORMAT, NOINIT,
NAME = N'SAMStore-Full Database Backup', SKIP, NOREWIND, NOUNLOAD,
STATS = 10
GO
```

2. Back up the transaction log:

   ```
   BACKUP LOG [SAMStore] TO DISK = N'C:\Program Files\Microsoft SQL
   Server\MSSQL.1\MSSQL\Backup\SAMStore_log.bak' WITH NOFORMAT, NOINIT,
   NAME = N'SAMStore-Transaction Log  Backup', SKIP, NOREWIND, NOUNLOAD,
   STATS = 10
   GO
   ```

3. Shrink the size of the log file:

   ```
   DBCC SHRINKFILE (N'SAMStore_log', 100) WITH NO_INFOMSGS
   ```

   SAMStore_log

   Specifies the logical transaction log file name.

   Sets the file size to 100MB. You can make it above or below this value depending on your disk space availability.

Error with Browser-Based UIs

Symptom:

Users are unable to access browser-based UIs such as the Dashboard, Mobile Dashboard, and USM Web View. The browser either indicates the page cannot be displayed, the certificate is invalid, or something similar.

Solution:

If you are using Windows XP/2003 clients through HTTPS, Microsoft provides a fix.

http://support.microsoft.com/default.aspx?scid=kb;EN-US;938397

All users must install this fix for their client.

Resolve an SA Store Database Connection Failure

Symptom:

I received an email notification that CA SOI has detected an SA Store Database connection failure.

Solution:

You set email notifications for database failures (see page 52).

1. Verify that the server is configured correctly and functioning outside of CA SOI.
2. Verify that the SA Store connection is working correctly using the DB Connectivity debug page. There are debug pages for the SA Manager server (see page 15) and for the UI server (see page 18):
    a. For each server, run the DB Connectivity report.
    b. View the report and review the following information:
        - The database connection, which determines if the server can connect to the SA Store Database at all.
        - The query speed test, which determines how fast the underlying database structure can respond to a simple query without accessing the database tables.
3. If the SA Manager server is offline and comes back online, CA SOI should detect the connection. If CA SOI is not connecting to the server, restart the SOI Application Manager service.

Resolve a Third-Party Server Connection Failure

Symptom:

I received an email notification that CA SOI has detected a third-party server connection failure.

Solution:

You previously set email notifications for third-party server failures (see page 52).

Follow these steps:

1. Verify that the server is configured correctly and functioning outside of CA SOI.
2. If the server is offline and comes back online, CA SOI detects the connection. If CA SOI is not connecting to the server, restart the SA Application Manager service.

SA Manager Crashing on Startup or Dumping Memory and Performing Slowly

Symptom:

I notice that either the SA Manager crashes when I restart the service or the SA Manager is dumping memory and performing slowly.

Solution:

There is a known issue where the SA Manager is either crashing at startup or dumping memory and performing slowly.

The SA Manager is trying to read the following file into memory:

SOI_HOMEI\tomcat\webapps\sam\console\logs\client.log

The problem is that the file has grown very large.

Follow these steps:

1. Stop the SA Manager service (CA SAM Application Server).
2. Delete the client.log file.
3. Restart the SA Manager service.SA Manager Crashing on Startup or Dumping Memory and Performing Slowly

[WrapperStartStopAppMain] Warning

Symptom:

I have entries in the SA Manager log (soimgr.log) and the UI Server log (soiuis.log) with warnings similar to the following examples:

```
2013-10-15 11:23:32,547 WARN  [WrapperStartStopAppMain]
config.ConfigurationFactory.parseConfiguration(133)  - 2013/10/15 11:23:32:538 EDT
[WARN] ConfigurationFactory - No configuration found. Configuring ehcache from
ehcache-failsafe.xml  found in the classpath:
jar:file:/E:/CA/SOI/wso2registry/repository/components/plugins/ehcache-1.5.0.wso2
v1.jar!/ehcache-failsafe.xml
```

```
2013-10-15 11:23:33,139 WARN  [WrapperStartStopAppMain]
config.ConfigurationFactory.parseConfiguration(133)  - 2013/10/15 11:23:33:138 EDT
[WARN] ConfigurationFactory - No configuration found. Configuring ehcache from
ehcache-failsafe.xml  found in the classpath:
jar:file:/E:/CA/SOI/wso2registry/repository/components/plugins/ehcache-1.5.0.wso2
v1.jar!/ehcache-failsafe.xml
```

```
2013-10-15 11:23:33,198 WARN  [WrapperStartStopAppMain]
ehcache.CacheManager.detectAndFixDiskStorePathConflict(322)  - 2013/10/15
11:23:33:197 EDT [WARN] CacheManager - Creating a new instance of CacheManager using
the diskStorePath "../../samui/temp" which is already used by an existing
CacheManager.

The source of the configuration was classpath.

The diskStore path for this CacheManager will be set to
../../samui/temp\ehcache_auto_created_1381850613197.

To avoid this warning consider using the CacheManager factory methods to create a
singleton CacheManager or specifying a separate ehcache configuration (ehcache.xml)
for each CacheManager instance.
```

Solution:

These warning messages generates when you restart the SA Manager and UI Server services. Ignore the warnings.

SOI Toolbox Troubleshooting

The troubleshooting topics in this section relate to the CA SOI Toolbox.

Toolbox Fails to Run

Symptom:

Every time that I try to run the CA SOI Toolbox, I receive a message similar to *The system cannot execute the specified program* message.

Solution:

Check the Windows Event Log for an *Event Properties - Event 33, SideBySide* message. If you find this event in your log, download and install the Microsoft Visual C++ 2008 Redistributable Package (x86).

USM Web View Troubleshooting

The troubleshooting topics in this section relate to the USM Web View application.

USM Web View Does Not Display All CIs

Symptom:

When I perform a search in USM Web View, I do not see all CIs that the CA SOI Connectors (Plug-ins) import.

Solution:

CIs are not imported from CA SOI into the CA Catalyst Database until the CIs are modeled as part of a CA SOI service. Once a CI becomes part of a CA SOI service, a projection is created and published to the CA Catalyst Persistence Store through the CA SOI CA Catalyst Connector.

If the CI is part of a modeled service, view the SOIConnector.log to verify that a projection was received. Also, see the invalidCIs.log to determine if the CI was rejected for some reason.

USM Web View Search Returns Incorrect Results

Symptom:

When I perform a search in USM Web View, one or both of the following events occur:

- Web View interface full text search does not find a few CIs, but the CIs are in the database and can be accessed through Browse.
- Or, Web View interface full text search shows few CIs that have been already deleted. The CIs are not accessible through Browse.

However, after I perform a reindex, the CIs are correctly found using full text search.

Solution:

To avoid potential search problems in USM Web View, synchronize the time on all machines where CA SOI and CA Catalyst are installed. Either configure the machines in the same Windows Server domain (so the domain controller synchronizes the time) or synchronize over Network Time Protocol (NTP).

The items that are created, updated, and modified in the CA Catalyst database are continuously indexed. The items are accessible using the full text search. The process that indexes them recognizes these items by a timestamp. If the machines are not time-synchronized, it is possible that some older create/update/delete timestamp is inserted after a newer one. If the indexer process ran between these two inserts, the older item is ignored and therefore unavailable (or still available after deletion) in the full text search.