IBM Tivoli Composite Application Manager for SOA
7.2 Fix Pack 1 (updated November 2015)

IBM Tivoli Composite Application Manager for SOA WSRR Integration Guide

IBM

IBM Tivoli Composite Application Manager for SOA
7.2 Fix Pack 1 (updated November 2015)

IBM Tivoli Composite Application Manager for SOA WSRR Integration Guide

IBM

Edition Notice

This edition applies to version 7.2 Fix Pack 1 of IBM Tivoli Composite Application Manager for SOA and to all subsequent releases and modifications until otherwise indicated in new editions.

Contents

Figures

About this publication

This publication provides information about integrating ITCAM for SOA version 7.2 or later with WebSphere® Service Registry and Repository version 7.5 or later so that ITCAM for SOA monitors services registered in WSRR and provides feedback to WSRR each time a policy breach of one of the registered services occurs.

Intended audience

This publication is for administrators or advanced users who want to integrate ITCAM for SOA with WSRR. The publication assumes that readers are familiar with the following topics:

- IBM® Tivoli® Monitoring 6.2.3 environment
- ITCAM for SOA version 7.2
- WSRR version 7.5
- Tivoli Enterprise Portal user interface
- Tivoli Enterprise Portal situation management
- Digital certificates for secure communication

Publications

This section lists publications in the product library and related documents. It also describes how to access Tivoli publications online and how to order Tivoli publications.

ITCAM for Applications library for ITCAM for SOA

The following publications are included in the ITCAM for Applications library, available in the ITCAM for Applications Information Center:

- *IBM Tivoli Composite Application Manager for SOA Installation Guide*

  Provides an overview of the IBM Tivoli Management Services environment and the planning information and procedures you need to install and upgrade the application support files and the monitoring agent in a distributed operating system environment.

  This guide also includes procedures for configuring support for the service-to-service topology function, including creating databases and configuring SOA Domain Management Server and Tivoli Common Object Repository in your Tivoli Enterprise Portal Server environment.

  This guide also includes procedures for enabling and disabling the various supported runtime environments for data collection by the ITCAM for SOA, version 7.2 monitoring agent, and optional administrative tasks to further configure your installation.

- *IBM Tivoli Composite Application Manager for SOA User's Guide*

  Provides information on monitoring and managing resources in the Tivoli Enterprise Portal environment, including details about Take Action commands, situations, workspaces and views, including service-to-service topology workspaces and views. Some problem determination information about the various components of ITCAM for SOA is also provided, as well as information

about log files and informational, warning, and error messages. This publication complements the Tivoli Enterprise Portal online help information for this monitoring agent.

- *IBM Tivoli Composite Application Manager for SOA Tools*

  Provides information about installing and using the IBM Web Services Navigator, an Eclipse based plugin for extracting services information that has been collected by monitoring agents and stored, either locally or in a historical database. This tool provides the capability to retrieve historical metric data from a connected database, or assemble several locally stored metric and content log files, and display the resulting data in several views to assist a services architect in visualizing relationships between services.

- *IBM Tivoli Composite Application Manager for Discovery Library Adapters Guide*

  Provides information about installing and running the following discovery library adapters (DLAs) provided with ITCAM for SOA: WebSphere Service Registry and Repository Discovery Library Adapter, Business Process Execution Language for Web Services Discovery Library Adapter, and IBM Tivoli Composite Application Manager for SOA Discovery Library Adapter.

- *IBM Tivoli Composite Application Manager for SOA Troubleshooting Guide*

  Provides information about recovering from problems that you might encounter while installing, configuring, and using the product. Typical problem scenarios are described, and recovery procedures are provided. Error messages for the product are also documented in this guide.

- *IBM Tivoli Composite Application Manager for SOA WSRR Integration Guide*

  Provides information about integrating ITCAM for SOA version 7.2 with WebSphere Services Registry and Repository version 7.5 or later. The procedure for subscribing to WSRR events related to service-level definitions and the procedure for creating and deploying an SDMS configuration file is documented. The configuration file defines the rules for processing WSRR events in SDMS. Based on these rules, situations are automatically created, updated, or deleted by IBM Tivoli Monitoring when a lifecycle changes notification is received from WSRR.

- *IBM Tivoli Composite Application Manager for SOA BPM Monitoring Deployment Guide*

  Provides information about implementing an IBM BPM monitoring solution.

- *IBM Tivoli Composite Application Manager for SOA Reports Guide*

  Provides information about installing and using ITCAM for SOA Reports.

Related publications

The following documentation also provides useful information:

- IBM Tivoli Documentation Central:

  Information about IBM Tivoli Documentation is provided on the following website:

  https://www.ibm.com/developerworks/community/wikis/home?lang=en#!/ wiki/Tivoli Documentation Central

- IBM WebSphere Application Server:

  Information about IBM WebSphere Application Server is provided on the following website:

  http://www.ibm.com/software/webservers/appserv/was/library/

- ITCAM for Application Diagnostics library:

Information about ITCAM for Application Diagnostics Managing Server is provided on the following website:

http://publib.boulder.ibm.com/infocenter/tivihelp/v24r1/index.jsp?topic=%2Fcom.ibm.itcamfad.doc_7101%2Fic-homepage.html

- IBM DB2®:

Information about IBM DB2 is provided on the following website:

http://www.ibm.com/software/data/sw-library/

Accessing terminology online

The IBM Terminology website consolidates the terminology from IBM product libraries in one convenient location. You can access the Terminology website at http://www.ibm.com/software/globalization/terminology .

Accessing publications online

The documentation CD contains the publications that are in the product library. The format of the publications is PDF, HTML, or both.

IBM posts publications for this and all other Tivoli products, as they become available and whenever they are updated, to the Tivoli Documentation Central website at https://www.ibm.com/developerworks/community/wikis/home?lang=en#!/wiki/Tivoli Documentation Central

Important: If you print PDF documents on other than letter-sized paper, set the option in the **File ▸ Print** window that allows Adobe Reader to print letter-sized pages on your local paper.

Ordering publications

You can order many Tivoli publications online at: http://www.ibm.com/e-business/weblink/publications/servlet/pbi.wss.

You can also order by telephone by calling one of these numbers:

- In the United States: 800-879-2755
- In Canada: 800-426-4968

In other countries, contact your software account representative to order Tivoli publications. To locate the telephone number of your local representative, perform the following steps:

1. Go to http://www.ibm.com/e-business/weblink/publications/servlet/pbi.wss
2. Select your country from the list and click **Go**.
3. Click **About this site** in the main panel to see an information page that includes the telephone number of your local representative.

Accessibility

Accessibility features help users with a physical disability, such as restricted mobility or limited vision, to use software products successfully. With this product, you can use assistive technologies to hear and navigate the interface. You can also use the keyboard instead of the mouse to operate all features of the graphical user interface.

For additional information, see Appendix A, Accessibility," on page 131.

Application Performance Management community on Service Management Connect

Connect, learn, and share with Service Management professionals: product support technical experts who provide their perspectives and expertise.

Access Service Management Connect at https://www.ibm.com/developerworks/servicemanagement/apm/index.html. Use Service Management Connect in the following ways:

- Become involved with transparent development, an ongoing, open engagement between other users and IBM developers of Tivoli products. You can access early designs, sprint demonstrations, product roadmaps, and prerelease code.
- Connect one-on-one with the experts to collaborate and network about Tivoli and the Application Performance Management community.
- Read blogs to benefit from the expertise and experience of others.
- Use wikis and forums to collaborate with the broader user community.

Tivoli technical training

For Tivoli technical training information, refer to the following IBM Tivoli Education website:

http://www.ibm.com/software/tivoli/education/

Tivoli user groups

Tivoli user groups are independent, user-run membership organizations that provide Tivoli users with information to assist them in the implementation of Tivoli Software solutions. Through these groups, members can share information and learn from the knowledge and experience of other Tivoli users. For more information about Tivoli Users Group, see www.tivoli-ug.org.

Support information

If you have a problem with your IBM software, you want to resolve it quickly. IBM provides the following ways for you to obtain the support you need:

Online
> Access the IBM Software Support site at http://www.ibm.com/software/support/probsub.html .

Troubleshooting Guide
> For more information about resolving problems, see the *IBM Tivoli Composite Application Manager for SOA Troubleshooting Guide*.

Conventions used in this publication

This publication uses several conventions for special terms and actions, operating system-dependent commands and paths, and margin graphics.

Typeface conventions

This publication uses the following typeface conventions:

Bold

- Lowercase commands and mixed case commands that are otherwise difficult to distinguish from surrounding text
- Interface controls (check boxes, push buttons, radio buttons, spin buttons, fields, folders, icons, list boxes, items inside list boxes, multicolumn lists, containers, menu choices, menu names, tabs, property sheets), labels (such as **Tip:**, and **Operating system considerations**:)
- Keywords and parameters in text

Italic

- Citations (examples: titles of publications, diskettes, and CDs
- Words defined in text (example: a nonswitched line is called a *point-to-point line*)
- Emphasis of words and letters (words as words example: "Use the word *that* to introduce a restrictive clause."; letters as letters example: "The LUN address must start with the letter *L*.")
- New terms in text (except in a definition list): a *view* is a frame in a workspace that contains data.
- Variables and values you must provide: ... where *myname* represents....

Monospace

- Examples and code examples
- File names, programming keywords, and other elements that are difficult to distinguish from surrounding text
- Message text and prompts addressed to the user
- Text that the user must type
- Values for arguments or command options

Operating system-dependent variables and paths

This guide refers to the following variables:

- *ITM_home*: the top-level directory for installation of IBM Tivoli Monitoring components. The default location is `C:\IBM\ITM` on Windows systems and `/opt/IBM/ITM` on Linux and UNIX systems?
- *KD4_DIR*: the directory of ITCAM for SOA on the Tivoli Enterprise Portal Server. The default locations are as follow:

  Windows systems: *ITM_home*`\CNPS\Products\KD4\latest`
  UNIX or **Linux systems**: *ITM_home*/*architecture*/`cq/Products/KD4/latest`

Chapter 1. Overview

ITCAM for SOA version 7.2 and later provides enhanced integration with WebSphere Service Registry and Repository (WSRR) version 7.5 or later. The integration allows ITCAM for SOA to monitor services registered in WSRR and to provide feedback to WSRR on policy breaches when they occur.

SOA Governance

SOA governance refers to the establishment of policies in an organization to ensure that services and composite applications deliver and maintain the quality of service levels expected of them. Service governance is part of SOA governance, and refers to a set of processes for identifying, building, deploying, and managing services. WSRR 7.5 is a service governance tool that stores and manages service descriptions.

WSRR encompasses both a service registry and a service repository:
- *service registry*: contains information about the services you use, plan to use, or need to be aware of within your organization or in other organizations. Using WSRR, you can publish metadata (for example, interfaces and operations) associated with the functions of a service. You can also publish metadata, for example, service-level definitions (SLDs), associated with the non-functional requirements of the service.
- *service repository*: stores, manages, and assigns a version number to service metadata.

In WSRR, a service defined from a business perspective is referred to as a capability. For each service, one or several SLDs are created. SLDs are used to specify both functional and nonfunctional requirements of a service. A policy, attached to the SLD, is used to define the quality of service requirements of the SLD. One or several policies are attached to an SLD. A service endpoint, associated with a policy attached to an SLD, defines how consumers of the service can physically connect to the service.

Governance enablement profile

WSRR installs and activates a default governance enablement profile as part of its standard installation. In WSRR, the profile is used to manage services from the initial specification of the service through to the deployment of the service into production. It contains a predefined set of states and transitions that can be applied to service artefacts such as SLDs, policies, service operations, and service endpoints.

For a description of the set of states and transitions of the SOA life cycle, the SLD life cycle, and the endpoint life cycle in the default governance enablement profile, see the WSRR Information Center:http://publib.boulder.ibm.com/infocenter/sr/v7r5/topic/com.ibm.sr.doc/rwsr_gep_life_cycles.html:

ITCAM for SOA

ITCAM for SOA provides software and integrated tools to monitor, manage, and control the web services layer of the IT architecture. It tracks the performance of

web services requests through application servers provided by IBM, such as WebSphere Application Server, DataPower®, and other SOA components provided by other organization such as SAP NetWeaver and JBoss. ITCAM for SOA has two primary integration points with WSRR:

1. ITCAM for SOA can be used discover and manage services that are registered in WSRR. ITCAM for SOA compares the services it observes in runtime environments against the services registered in WSRR to identify services that are not being used and to identify rogue services. ITCAM for SOA displays the registered services in topology views. ITCAM for SOA uses a Discovery Library Adapter (DLA) to extract services data from WSRR. For more information about this particular integration point, see the *IBM Tivoli Composite Application Manager for SOA Discovery Library Adapters* guide.

2. ITCAM for SOA uses IBM Tivoli Monitoring to automatically create situations when services and service-related entities are modified in WSRR. The situations are used to track policy conditions that a service must meet, such as response time. ITCAM for SOA subscribes to events from WSRR. Each time an SLD, policy, service operation, or service endpoint changes its life cycle state, a notification is sent to ITCAM for SOA. IBM Tivoli Monitoring creates, modifies, or updates situations based on a subset of these states. When a policy condition is breached, ITCAM for SOA uses an event handler interface to report the situation to WSRR. When the WSRR receives the notification, it creates, updates, or deletes properties on a WSDL port or a SCA export associated with the service in the registry. This two-way communication path is the focus of this guide.

By default, ITCAM for SOA subscribes to all WSRR events. However, it creates, updates, or modifies situations only if the event indicates that specific transactions have occurred in WSRR. The type of transactions that trigger ITCAM for SOA to create, update, or delete a situation depend on the entity:

- For an SLD, IBM Tivoli Monitoring modifies situations when an SLD has been updated, approved, deprecated, superseded, or is no longer being governed. It modifies situations when a service policy has been attached to an SLD or removed from it.

- For a service policy, IBM Tivoli Monitoring modifies situations when a policy has been approved for production, updated, revoked, retired, or is no longer being governed.

- For a service operation, IBM Tivoli Monitoring modifies situations when a service operation is updated or deleted.

- For a service endpoint, IBM Tivoli Monitoring modifies situations when a service endpoint is brought online or offline, when a service endpoint is updated or deleted, or when it is no longer being governed.

Integration of ITCAM for SOA with WSRR

The following diagram displays the interaction between each of the WSRR and ITCAM for SOA components in the integration.
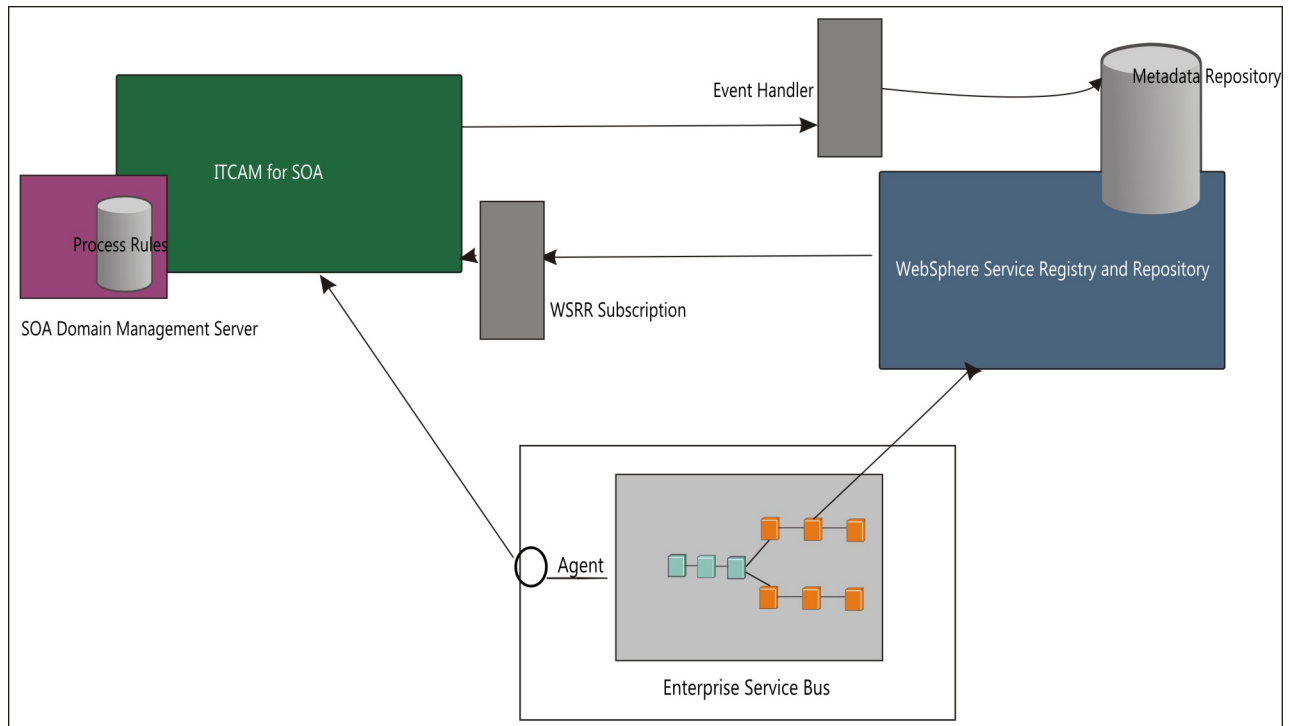
Figure 1. ITCAM for SOA and WSRR Integration

To use ITCAM for SOA to monitor and report on quality of service levels of registered services, you must subscribe ITCAM for SOA to WSRR events.

Next, you must configure ITCAM for SOA to process WSRR events published on a WSRR event subscription. For example, when the life cycle of an SLD transitions to a subscribable state, WSRR notifies ITCAM for SOA using the event subscription. When ITCAM for SOA receives this notification, it automatically retrieves policy information for the SLD from WSRR, and uses IBM Tivoli Monitoring to create a situation based on the policy. When WSRR notifies ITCAM for SOA of any changes to the SLD or any entities attached to the SLD, such as policies or service endpoints, IBM Tivoli Monitoring updates the situations accordingly. When an SLD is no longer being monitored by WSRR, IBM Tivoli Monitoring deletes the situations for the SLD.

Each time a situation is triggered or cleared, IBM Tivoli Monitoring generates an event. You must configure IBM Tivoli Monitoring to forward such events to WSRR. For more information about configuring event forwarding, see the *IBM Tivoli Monitoring information center*.

You must also configure the WSRR event handler to process these events. WSRR sets, updates, or clears properties on an WSDL port or an SCA export related to a service when it receives a notification that a situation has been triggered or cleared.

Prerequisites

The following software is required to integrate WSRR with ITCAM for SOA.
- ITCAM for SOA version 7.2 or later.
- WebSphere Service Registry and Repository version 7.5 or later

- IBM Tivoli Monitoring version 6.2.2 fix pack 3 or higher or version 6.2.3 and its fix packs

See the Software product compatibility reports website to generate various reports that are related to product and component requirements.

To view the system requirements for server-side components in ITCAM for SOA version 7.2 and later, see the Server-side components detailed system requirements report.

To view the system requirements for agent-side components in ITCAM for SOA version 7.2 and later, see the Agent-side components detailed system requirements report.

Chapter 2. Configuring the WSRR instance

You must make configuration changes to a WSRR instance to enable integration with ITCAM for SOA.

To establish SSL communication between WSRR and IBM Tivoli Monitoring, you must import the IBM Tivoli Monitoring SSL certificate into WSRR. You must have access to the WSRR administrative console to import the certificate.

To configure IBM Tivoli Monitoring to receive notification events from WSRR, you must create an authentication alias in WSRR for an IBM Tivoli Monitoring administrative user. To create the authentication alias, you must have access to the administrative console of the WebSphere Application Server instance running the WSRR application.

To enable WSRR to publish HTTP post notifications on a HTTP Post subscription (used for communication with Tivoli Monitoring), you must configure the HTTP Post Notifier Plugin and the Subscription Notifier Plugin Scheduler. You must be able to access WSRR as a user with the configuration role assigned to configure both plug-ins.

Importing the IBM Tivoli Monitoring SSL certificate

You must import the IBM Tivoli Monitoring SSL certificate into WSRR to enable secure communication between ITCAM for SOA and WSRR.

About this task

Complete the following procedure to import the Tivoli Monitoring SSL certificate into WSRR.

Procedure

1. Log on to the administrative console for the WebSphere Application Server instance that is running the WSRR application.
2. Select **Security** > **SSL certificate and keystore management**.
3. Under **Related Items**, select **Key stores and certificates**.
4. In the list of key stores, select **NodeDefaultTrustStore**.
5. Under **Additional Properties**, select **Signer Certificates**.
6. Click the **Retrieve from port** button. The system displays the entry fields for retrieving a certificate from a network server.
7. Enter the following information:
   - **Host**: The host name or IP address of the Tivoli Enterprise Portal Server.
   - **Port**: The configured HTTPS transport port of the Tivoli Enterprise Portal Server. The default HTTPS transport port is 15211.
   - **Alias**: The alias that WSRR uses for the certificate. This alias must be unique for this WSRR instance. For example, itm_*host_port*.

   To determine the HTTPS transport port number, see the following file on the Tivoli Enterprise Portal Server host:

- On Windows systems, *ITM_home*\CNPSJ\profiles\ITMServer\logs\AboutThisProfile.txt
- On Linux and UNIX systems, *ITM_home*/*architecture*/iw/profiles/ITMProfile/logs/AboutThisProfile.txt

8. Click the **Retrieve signer information** button. WSRR retrieves and displays the SSL certificate.
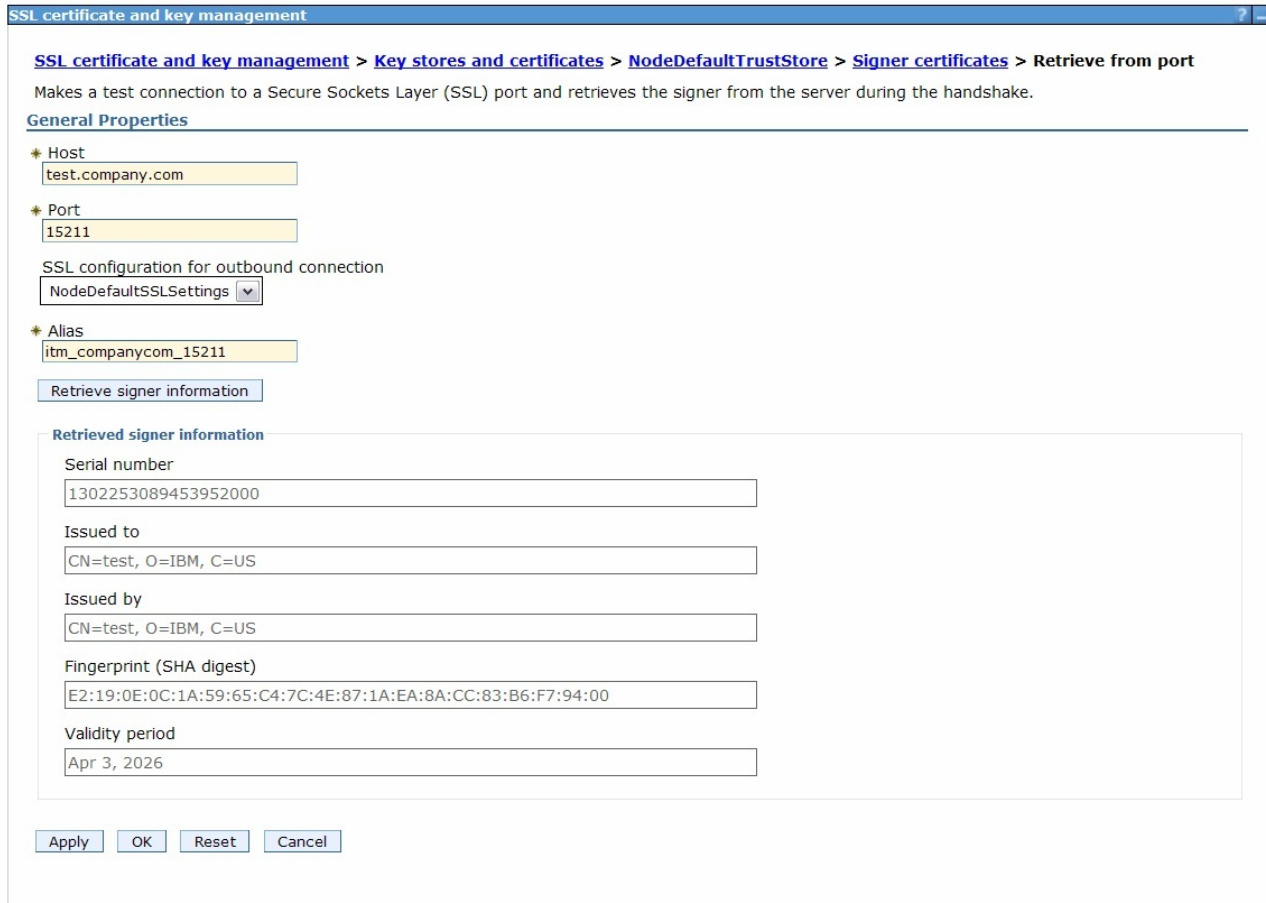
Figure 2. SSL certificate information

9. Click **OK**. When prompted, click **Save**.

Creating an authentication alias for an IBM Tivoli Monitoring user

To enable IBM Tivoli Monitoring to receive event notifications from WSRR, you must create an authentication alias in WSRR for an IBM Tivoli Monitoring administrative user.

About this task

Complete the following procedure to create an authentication alias in WSRR for an IBM Tivoli Monitoring user.

Procedure

1. Log in to the administrative console of the WebSphere Application Server instance that is running the WSRR application.

2. Select **Security** > **Global security**.

3. Under **Authentication**, expand **Java Authentication and Authorization Service**, then select **J2C authentication data**.

4. If the **Prefix new alias names with the node name of the cell** check box is selected, clear the check box.

5. Click **Apply**.

6. Click **New**.

7. Enter the following information:

   - **Alias**: The alias for the authentication data. You must use this alias in the WSRR subscription definition file (see Creating the subscription definition file″ on page 19).

     Important: On Linux and UNIX systems, the alias for the authentication must be in upper case.

   - **User ID**: The identifier for the IBM Tivoli Monitoring user with the administrative role. The user must have permission to start, stop, and modify situations.

   - **Password**: The password for the user.

   - **Description**: The description that WSRR displays for this alias.

8. Click **OK**. When prompted, click **Save**.

Configuring the Subscription Notifier Plugin Scheduler

WSRR uses the Subscription Notifier Plugin Scheduler to send events to ITCAM for SOA. You must ensure that the scheduler is configured correctly.

About this task

Complete the following procedure to configure the Subscription Notifier Plugin Scheduler.

Procedure

1. Log in to WSRR as a user with the configuration role assigned.

2. In the **Active Profile** menu, select **Scheduler**.

3. In the list of scheduler configurations, click **SubscriptionNotifierPluginScheduler**. The following page opens:
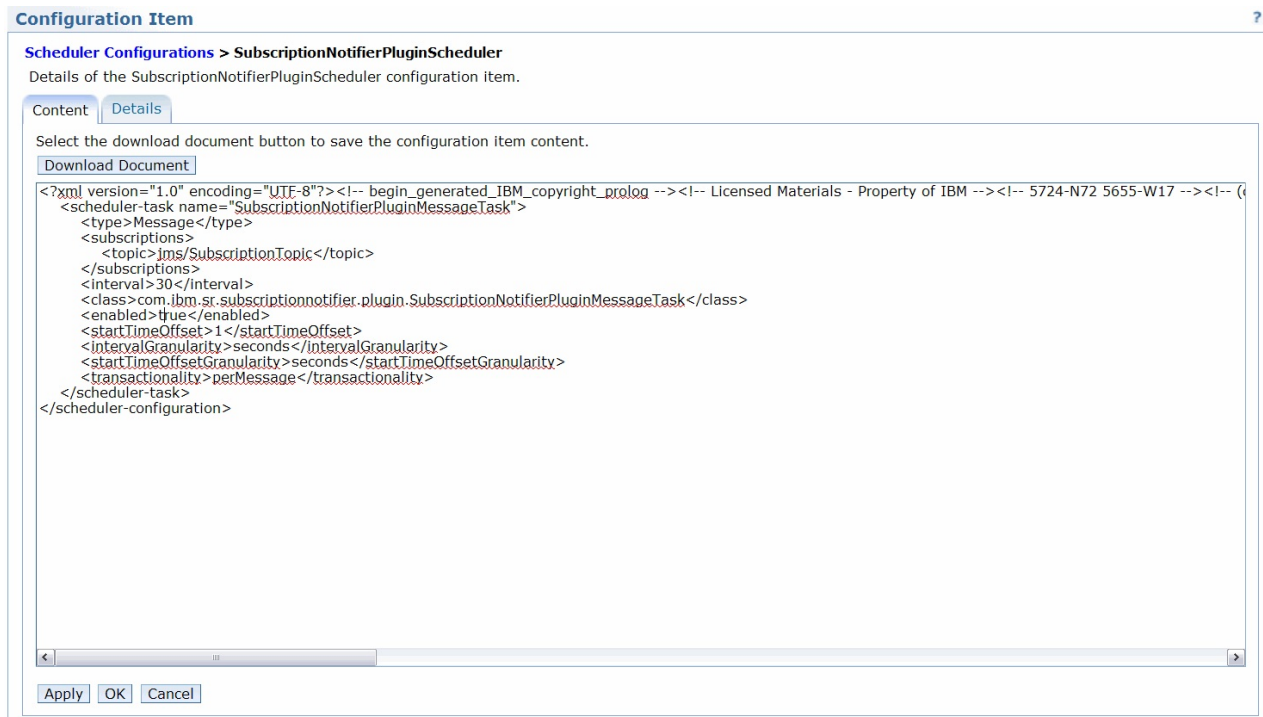
Figure 3. SubscriptionNotifierPluginConfiguration configuration

4. In the XML editing field, under the <scheduler-configuration> tag, ensure that the following values are set within several tags:

```
<interval>30</interval>

<enabled>true</enabled>
<startTimeOffset>1</startTimeOffset>
<intervalGranularity>seconds</intervalGranularity>
<startTimeOffsetGranularity>seconds</startTimeOffsetGranularity>
 <transactionality>perMessage</transactionality>
```

Use these exact values without modifying them, unless directed by IBM Support. Do not modify the values in other tags.

5. Click **OK** to apply your changes.

Configuring the HTTP Post Notifier plugin

WSRR uses the HTTP Post Notifier plugin to send events to ITCAM for SOA. You must ensure that the notifier plug-in is configured correctly.

About this task

Complete the following procedure to configure the HTTP Post Notifier plugin.

Procedure

1. Log in to WSRR as a user with the configuration role assigned.
2. In the **Active Profile** menu, select **Notifiers** > **Subscription Notifier**.
3. In the list of subscription notifier configurations, click **SubscriptionNotifierPluginConfiguration**. The following page opens:
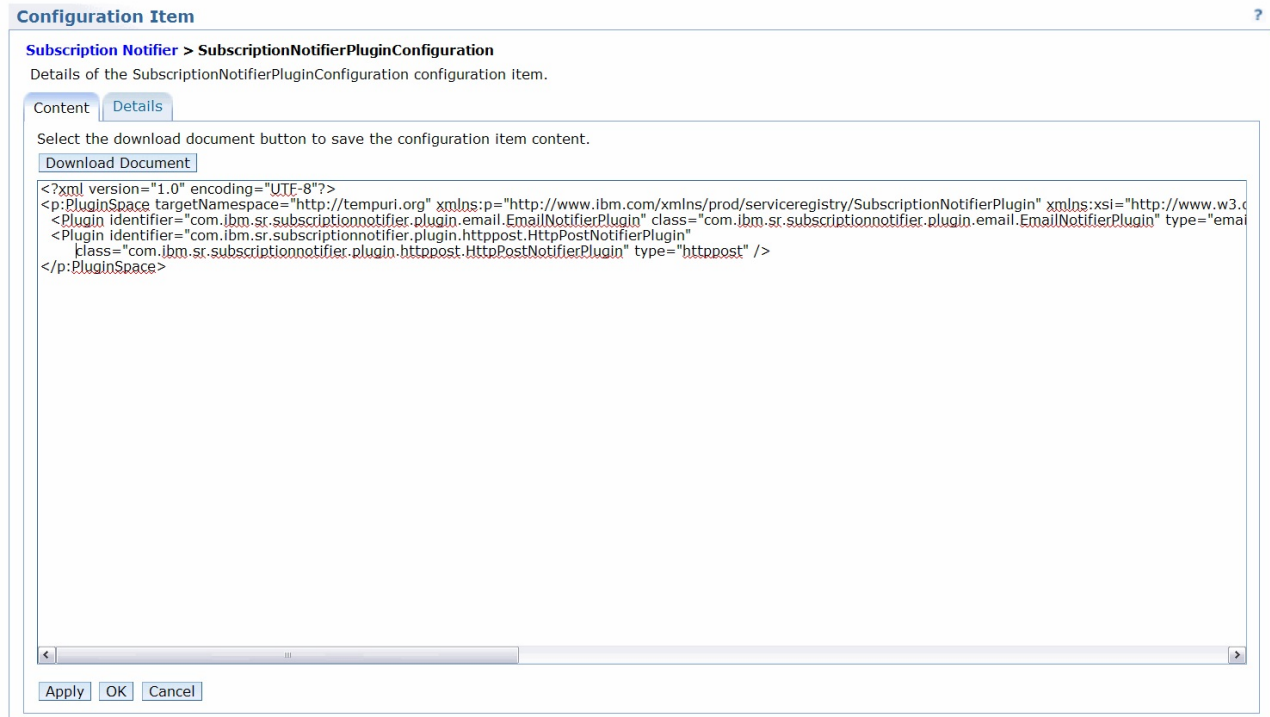
Figure 4. SubscriptionNotifierPluginScheduler configuration

4. Find the following element and ensure that it is not commented out:

```
<Plugin
 identifier="com.ibm.sr.subscriptionnotifier.plugin.httppost.HttpPostNotifierPlugin
 class="com.ibm.sr.subscriptionnotifier.plugin.httppost.HttpPostNotifierPlugin"
 type="httppost" /></p:PluginSpace>
```

Tip: Any XML text surrounded by `<!--` and `-->` is commented out. In the following example, the element is commented out:

```
<!--<Plugin
 identifier="com.ibm.sr.subscriptionnotifier.plugin.httppost.HttpPostNotifierPlugin
 class="com.ibm.sr.subscriptionnotifier.plugin.httppost.HttpPostNotifierPlugin"
 type="httppost" /></p:PluginSpace>-->
```

Remove the `<!--` and the `-->` strings to uncomment the element.

5. Click **OK**.

Chapter 3. Configuring IBM Tivoli Monitoring

You must make configuration changes to IBM Tivoli Monitoring to enable it to communicate with WSRR. You must have access to the Tivoli Enterprise Portal Server administration console to make the configuration changes.

Importing the WSRR SSL certificate on the portal server

To enable SSL communication between a WSRR and IBM Tivoli Monitoring, you must import the SSL certificate of the WSRR into the master Tivoli Enterprise Portal Server. You do not have to import the certificate into other Tivoli Enterprise Portal Servers.

About this task

Complete the following procedure to import the WSRR SSL certificate into the master Tivoli Enterprise Portal Server.

Procedure

1. If the Tivoli Enterprise Portal Server administration console is disabled, enable it. For details, see the IBM Tivoli Monitoring Information Center at http://publib.boulder.ibm.com/infocenter/tivihelp/v15r1/topic/ com.ibm.itm.doc_6.2.3/welcome.htm; search for Starting the TEPS/e administration console˝and select the topic named Starting the TEPS/e administration console˝ from the search results.

2. Log in to the Tivoli Enterprise Portal Server administration console. The URL for this console is `https://hostname:port/ibm/console/logon.jsp`

   hostname is the Tivoli Enterprise Portal Server host name.

   port is the Tivoli Enterprise Portal Server Administrative console secure port.

   To determine the port number, see the following file on the Tivoli Enterprise Portal Server host:

   - On Windows systems, `ITM_home\CNPSJ\profiles\ITMServer\logs\ AboutThisProfile.txt`

   - On Linux and UNIX systems, `ITM_home/architecture/iw/profiles/ ITMProfile/logs/AboutThisProfile.txt`

3. Select **Security** > **SSL certificate and keystore management**.

4. Under **Related Items**, select **Key stores and certificates**.

5. In the list of key stores, click **NodeDefaultTrustStore**.

6. Under **Additional Properties**, select **Signer certificates**.

7. Click the **Retrieve from port** button. The system displays the entry fields for retrieving a certificate from a network server.

8. Enter the following information:

   - **Host**: The host name or IP address of the server hosting the WSRR instance.

   - **Port**: The configured HTTPS transport port of the WSRR server instance.

   - **Alias**: The alias that IBM Tivoli Monitoring uses for the certificate. This alias must be unique for this Tivoli Enterprise Portal Server environment. For example, `wsrr_host_port`.

9. Click the **Retrieve signer information** button. WSRR retrieves the SSL certificate and displays it.
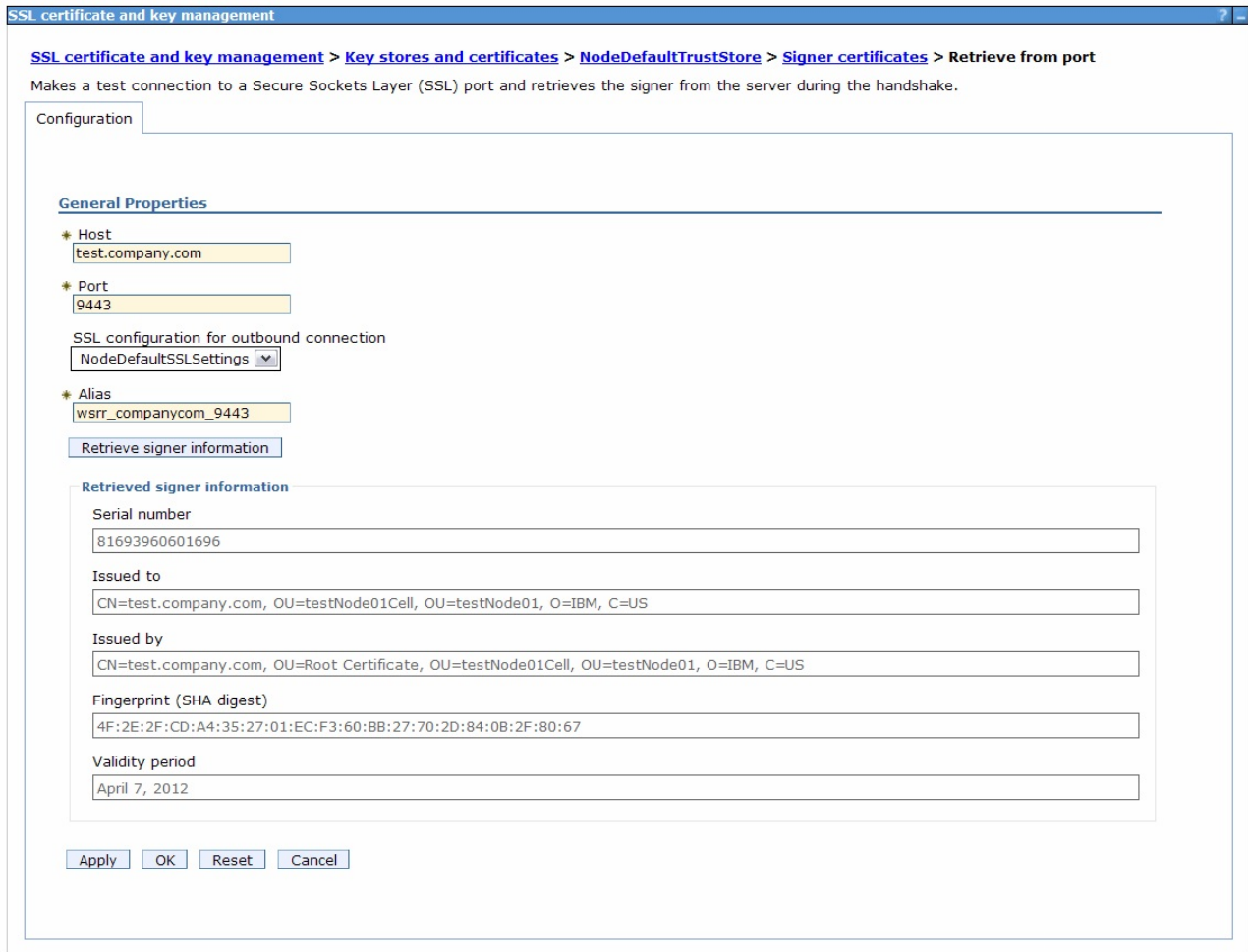
Figure 5. SSL certificate information

10. Click **OK**. When prompted, click **Save**.

Creating Take Action commands

You can reference Take Action commands in WSRR monitoring policies. For the reference to work, you might need to define the Take Action commands in Tivoli Monitoring.

In a WSRR monitoring policy, you can reference a Tivoli Monitoring Take Action command. To reference a Take Action command, use the <wsmon:SystemCommand> tag:

```
<wsmon:Action>
 <wsmon:ITM>
   <wsmon:SystemCommand>[value of SystemCommand></wsmon:SystemCommand>
 </wsmon:ITM>
</wsmon:Action>
```

When SDMS creates a situation for a WSRR monitoring policy, if the policy references a Take Action command this command is set for the situation. When the situation is triggered, Tivoli Monitoring executes the command.

Standard Take Action commands exist for every agent and are described in the documentation for each agent. Alternatively. you can create a custom Take Action command. For more information, see the topic on creating Take Action commands in the *Tivoli Enterprise Portal User's Guide*.

Configuring EIF event destinations

You can use the Tivoli Monitoring Event Integration Facility (EIF) to forward events when the situations for WSRR policies trigger. To use this functionality, you must configure EIF event destinations in Tivoli Monitoring.

Every EIF event destination must have an ID, which is a number in the range of 1 to 999. Every destination must have a unique ID.

To configure EIF event destinations, you can use the following commands through `tacmd`, the Tivoli Monitoring command line utility. Fir detailed information about the commands, see the *IBM Tivoli Monitoring Command Reference*.

- To log in to the server before executing any other commands, use `tacmd login`.
- To view the list of event destinations and their IDs, use `tacmd listEventDest`.
- To view the details for an event destination, use `tacmd viewEventDest`.
- To create an event destination and set its ID, use `tacmd createEventDest`.
- To delete an event destination, use `tacmd deleteEventDest`.
- To log out of the server after executing commands, use `tacmd logout`.

To use event forwarding, modify the following property attributes within the <situation-configuration> tag:

```
<property name="situation.tec.forwarding" value="true"/>
<property name="situation.tec.destination" value="IDs"/>
```

IDs is the event destination or comma-separated list of event destinations. For example, 14 or 11,20.

For details about the property settings, see Situation parameters" on page 34.

Chapter 4. Creating and deploying the WSRR SDMS configuration file

To enable WSRR to integrate with ITCAM for SOA, you must provide and deploy the WSRR SOA Domain Management Server (SDMS) configuration file. The SOA Domain Management Server is one of the components of the ITCAM for SOA that is used to retrieve services information from the WSRR. This WSRR SDMS configuration file defines how ITCAM for SOA must process WSRR notification events.

The WSRR SDMS configuration file defines process rules that govern creating, updating, starting, stopping, and deleting ITCAM for SOA situations according to the progress of SLDs, policies, service operations, and service endpoints through WSRR life cycles.

To create this file, you must save a copy of the WSRR configuration template file and modify its values. Then run a script to deploy the WSRR SDMS configuration file.

Creating the WSRR SDMS configuration file

You must create the WSRR SDMS configuration file. Templates for this file for use with WSRR versions 7.5 and 8.x are included with ITCAM for SOA version 7.2. You must update the template with values that are specific to your environment.

About this task

The WSRR SDMS configuration file template specifies that ITCAM for SOA must create situations for all SLDs in a subscribable state and policies in a monitored state. For a detailed definition of the default process, see Default process overview" on page 29.

Important: The values in the template are based on the default WSRR governance enablement profile. If WSRR is configured with a different governance enablement profile, you must customize the WSRR SDMS configuration file accordingly. See Customizing situation management" on page 55.

Procedure

1. Make a copy of the following file template:
   - If you are using WSRR version 7.5, *KD4_DIR*/bin/ wsrr_sdms_config_template.xml
   - If you are using WSRR version 8.x, *KD4_DIR*/bin/ wsrr_sdms_config_template_8.0.xml

   Save the copy of the file in any directory as wsrr_sdms_config.xml, and open the file in a text editor.

   Limitation: The full path to the file must not contain spaces. This is a limitation of the current version.

2. In the opened file, replace the following strings (macros) with actual values for your environment:

Table 1. Macros that you must replace in the `wsrr_sdms_config.xml`

Macro	Description
ITM_USERNAME	The IBM Tivoli Monitoring administrator user name. Set this value to the user ID that is set in Creating an authentication alias for an IBM Tivoli Monitoring user" on page 6. **Important:** On Linux and UNIX systems, the user name must be in upper case.
ITM_PASSWORD	The IBM Tivoli Monitoring administrator password. Set this value to the password set in Creating an authentication alias for an IBM Tivoli Monitoring user" on page 6.
WSRR_HOST	The host name of the server where WSRR is installed.
WSRR_PORT	The administration port of WSRR.
WSRR_USERNAME	The name of a WSRR administrative user.
WSRR_PASSWORD	The password for the WSRR administrative user.
CORRELATION_ID	A string value that is used to correlate the event published by WSRR with the subscription created in WSRR by IBM Tivoli Monitoring. You can use any string, for example, `CorrelationId_1`. This value and the `_correlationId` value in the subscription XML definition file (see Creating the subscription definition file" on page 19) must be the same. The value must be unique in your environment.
SECURITY_TOKEN	A string value that is used to validate that the events published by WSRR are consistent with the subscription created in WSRR by IBM Tivoli Monitoring. You can use any string, for example, `SecurityToken_1`. This value and the `_endPointSecurityToken` value in the subscription XML definition file (see Creating the subscription definition file" on page 19) must be the same. The value must be unique in your environment.
NAME	A string value representing the WSRR instance name. You can use any string for this value. SDMS uses this string in the names it assigns to situations that it creates. You must not change this name after it is set. **Important:** Do not replace the `Name` macro globally. Replace each occurrence of the `Name` macro individually.

Macro	Description
SUBSCRIPTION_NAME	A string value representing the name of the subscription created by IBM Tivoli Monitoring in WSRR. You can use any string, for example, `Subscription_1`. This value and the `name` value in the subscription XML definition file (see Creating the subscription definition file″ on page 19) must be the same.

> **Important:** If several WSRR instances are deployed on the same node, you must also add the WSRR instance prefix to the WSRR instance definition in the <wsrr-instance> tag. When multiple WSRR instances are used in the same WebSphere Application Server cell, one must set a prefix during WSRR configuration. See WSRR instances″ on page 41.

> **Tip:** Record the values for CORRELATION_ID, SECURITY_TOKEN, and NAME values, as they are required for subsequent configuration steps.

3. Save and close the file.

Running the script to deploy the WSRR SDMS configuration file

You must run a script to deploy the WSRR SDMS configuration file. Run the script again each time that you change the file.

About this task

Complete the following procedure to run the deployment script for the WSRR SDMS configuration file.

Procedure

1. Change to the *KD4_DIR*/bin directory.
2. Run the following command:
   - On Windows systems: kd4WSRRSDMSConfiguration.bat *config_file_name arguments*
   - On Linux and UNIX systems: ./kd4WSRRSDMSConfiguration.sh *config_file_name arguments*

   Replace *config_file_name* with the fully qualified pathname of the wsrr_sdms_config.xml file. Use the optional command-line argument -resync *true* to synchronize all of the ITCAM for SOA situations with subscribable SLDs once the WSRR SDMS configuration file has been deployed.

> **Important:** When deploying the configuration file, the script uses the AES algorithm to encrypt the passwords both in the deployed copy and in the original file.

> **Limitation:** The full path to the WSRR SDMS configuration file must not contain any spaces. This is a limitation of the current version.

Example

Example of the output produced when the script is run without the optional argument -resync *true*:

```
C:\ITM\CNPS\Products\KD4\latest\bin>kd4WSRRSDMSConfiguration.bat c:\work\wsrr_sdms_config.xml
KD4DM0305I Loading the configuration XSD to validate the configuration file...
KD4DM0306I The configuration file, c:\work\wsrr_sdms_config.xml, is being validated...
KD4DM0307I The configuration file is valid.
KD4DM0309I Encrypting the passwords in the configuration file.
KD4DM0310I The updates to the configuration file have completed.
KD4DM0312I Proceeding to deploy the configuration changes in SDMS...
WASX7209I: Connected to process "ITMServer" on node ITMNode using SOAP connector;
   The type of process is: UnManagedProcess
WASX7303I: The following options are passed to the scripting environment and are available
   as arguments that are stored in the argv variable: "[c:\work\wsrr_sdms_config.xml]"
Update of KD4SDMS has started.
ADMA5009I: An application archive is extracted at
            C:\ITM\CNPSJ\profiles\ITMProfile\wstemp\wstemp\app_1302b3ca939\ext
ADMA5064I: FileMergeTask completed successfully for KD4SDMS.
ADMA5005I: The application KD4SDMS is configured in the WebSphere Application Server
repository.
ADMA5005I: The application KD4SDMS is configured in the WebSphere Application Server
repository.
ADMA5005I: The application KD4SDMS is configured in the WebSphere Application Server
repository.
ADMA5011I: The cleanup of the temp directory for application KD4SDMS is complete.
Update of KD4SDMS has ended.
```

Example of the output produced when the script is run with the optional argument -resync *true*:

```
C:\ITM\CNPS\Products\KD4\latest\bin>kd4WSRRSDMSConfiguration.bat
C:\work\wsrr_sdms_config.xml -resync true
KD4DM0305I Loading the configuration XSD to validate the configuration file...
KD4DM0306I The configuration file, C:\work\wsrr_sdms_config.xml, is being validated...
KD4DM0307I The configuration file is valid.
KD4DM0309I Encrypting the passwords in the configuration file.
KD4DM0310I The updates to the configuration file have completed.
KD4DM0312I Proceeding to deploy the configuration changes in SDMS...
WASX7209I: Connected to process "ITMServer" on node ITMNode using SOAP connector;
The type of process is: UnManagedProcess
WASX7303I: The following options are passed to the scripting environment
and are available as arguments that are stored in the argv variable:
"[c:\work\wsrr_sdms_config.xml]"
Update of KD4SDMS has started.
ADMA5009I: An application archive is extracted at
C:\ITM\CNPSJ\profiles\ITMProfile\wstemp\wstemp\app_1333584ca4b\ext
ADMA5064I: FileMergeTask completed successfully for KD4SDMS.
ADMA5005I: The application KD4SDMS is configured in the WebSphere Application Server
repository.
ADMA5005I: The application KD4SDMS is configured in the WebSphere Application Server
repository.
ADMA5005I: The application KD4SDMS is configured in the WebSphere Application Server
repository.
ADMA5011I: The cleanup of the temp directory for application KD4SDMS is complete.
Update of KD4SDMS has ended.
KD4DM0351I ITM situation synchronization started at 10/24/11 11:41 AM
KD4DM0352I ITM situation synchronization done    at 10/24/11 11:42 AM
```

Chapter 5. Creating the WSRR subscription

For ITCAM for SOA and WSRR to work together, a WSRR subscription is required. WSSR uses the subscription to send SLD, service, policy, and operation information to ITCAM for SOA. To create the subscription, you must create a subscription definition file, and then run the subscription script, supplying the name of this file.

For details on customizing the SLD subscription definition, refer to the WSRR information center at http://publib.boulder.ibm.com/infocenter/sr/v7r5/topic/com.ibm.sr.doc/cwsr_subscr_notif.html.

Creating the subscription definition file

The subscription definition file defines event types for a WSRR subscription, such as *create* and *update*. To create the subscription definition file, use the template that is provided with ITCAM for SOA. This template defines a single subscription for create, delete, update, transition, and remove governance event types.

About this task

To create a subscription definition file using the template, complete the following procedure.

Procedure

1. Make a copy of the following template file: `KD4_DIR`/bin/`wsrr_subscription_template.xml`. Save the copy in any directory as `wsrr_subscription.xml`, and open the file in a text editor. (You can also use another name that is easy to identify, such as `wsrr_subscription_instance.xml`, where *instance* is the instance name set during WSRR configuration).
2. There are a number of entries in this XML file that have the following form:

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

   Set the values for several properties, as listed in the following table:

Table 2. Properties that you must set in the `wsrr_subscription.xml` file

Property name	Value
name	The name for the subscription. WSRR displays this name in the list of subscriptions. You must set this value to the same string value as it used by the SUBSCRIPTION_NAME macro in the WSRR SDMS configuration file (see Creating the WSRR SDMS configuration file˝ on page 15).

Table 2. Properties that you must set in the `wsrr_subscription.xml` *file (continued)*

Property name	Value
`_endPointSecurityToken`	The security token. You must set this value to the same string value as used by the SECURITY_TOKEN macro in the WSRR SDMS configuration file (see Creating the WSRR SDMS configuration file″ on page 15). You can use any string value, for example, `SecurityToken_1`. If you create several subscriptions (whether to the same or different WSRR instances), use a unique security token for each subscription.
`_endPointSecurityAuthAlias`	The authentication alias. You must set this value to the alias set in Creating an authentication alias for an IBM Tivoli Monitoring user″ on page 6.
`_correlationID`	The correlation ID. You must set this value to the same string as the CORRELATION_ID macro in the WSRR SDMS configuration file (see Creating the WSRR SDMS configuration file″ on page 15). This can be any string, for example, `CorrelationId_1`. If you create several subscriptions (whether to the same or different WSRR instances), use a unique correlation ID for each subscription.
`_endPointReference`	An URL with the host name of theTivoli Enterprise Portal Server and the HTTP transport port configured on the Tivoli Enterprise Portal Server. To determine the port number, see the "HTTP transport port″ in following file on the Tivoli Enterprise Portal Server host: • On Windows systems, `ITM_home\CNPSJ\profiles\ITMProfile\ logs\AboutThisProfile.txt` • On Linux and UNIX systems, `ITM_home/architecture/iw/profiles/ ITMProfile/logs/AboutThisProfile.txt` Do not change the rest of the URL from the default value. For example: `http:// teps.company.com:15210/ com.ibm.management.soa.dms.wsrrsync .servlet/WSRRNotificationServlet`

Important: Do not change other settings in this file, unless you also customize the WSRR SDMS configuration file to handle different subscriptions (see Chapter 7, Customizing the integration process," on page 29). Refer to WSRR documentation at http://publib.boulder.ibm.com/infocenter/sr/v7r5/topic/ com.ibm.sr.doc/cwsr_subscr_notif.html for details on defining subscriptions.

Running the subscription script

To create the WSRR subscription for ITCAM for SOA, you must run the subscription script, supplying the name of the subscription definition file. If you modify the file, you must delete the subscription in WSRR and then run the script again.

About this task

Complete the following steps to run the subscription script.

Procedure

1. Change to the *KD4_DIR*/bin directory.
2. Run the following command:
   - On Windows systems, kd4WSRRSubscriber.bat *arguments*
   - On Linux and UNIX systems, ./kd4WSRRSubscriber.sh *arguments*

   Use the following arguments.

Table 3. Command-line arguments for the subscription script

Parameter name	Parameter value
-wsrrHost *host*	The name of the WSRR host.
-wsrrPort *port*	The WSRR port number.
-wsrrUsername *username*	The WSRR user name.
-wsrrPassword *password*	The WSRR password.
-wsrrSubscription *filename*	The fully qualified path name of the WSRR subscription definition XML file.
-operation create	(Optional) The type of operation. The create operation is the only option currently available.
-wsrrInstancePrefix *prefix*	(Optional) The WSRR instance prefix. When multiple WSRR instances are used in the same WebSphere Application Server cell, one must set a prefix during WSRR configuration. Use the prefix value that is defined in the <wsrr-instance> tag (see Creating the WSRR SDMS configuration file″ on page 15).
-wsrrSecure true|false	(Optional) True if WSRR is secured, that is, accessed via HTTPS. The default is true.
-wsrrAuthRealm *wsrrAuthRealm*	(Optional) The WSRR authentication realm.
-wsrrVersion *version*	(Optional) The WSRR version. The default is 7.5.
-useProxy true|false	(Optional) True if a proxy is used. The default is false.
-proxyHost *proxyHost*	The proxy host address (required only if useProxy is true).
-proxyPort *proxyPort*	The proxy port number (required only if useProxy is true).
-proxyUsername *proxyUsername*	(Optional) The proxy user name.

Table 3. Command-line arguments for the subscription script (continued)

Parameter name	Parameter value
-proxyPassword *proxyPassword*	(optional) The proxy password. If the password is an empty string, simply specify `-password`.
-proxyAuthRealm *proxyAuthRealm*	(Optional) The proxy authentication realm
-sslTimeout *sslTimeout*	(Optional) The SSL timeout in milliseconds. The default value is 60000.

Examples

The following commands create a notification subscription in the WSRR instance on the `wsrr.company.com` host, on port 9443, with the specified user name and password:

- On Windows systems:

```
kd4WSRRSubscriber.bat —wsrrHost wsrr.company.com —wsrrPort 9443 —wsrrSubscription
    C:\wsrr_subscription.xml —wsrrUsername admin —wsrrPassword adminpassword
```

- On Linux and UNIX systems:

```
./kd4WSRRSubscriber.sh —wsrrHost wsrr.company.com —wsrrPort 9443 —wsrrSubscription
    /home/itmadmin/wsrr_subscription.xml —wsrrUsername admin
    —wsrrPassword adminpassword
```

If an HTTP proxy at `proxy.company.com` is required for the ITCAM for SOA host to access the WSRR instance, and the proxy server requires authentication using a user name and password, the following commands are required:

- On Windows systems:

```
kd4WSRRSubscriber.bat —wsrrHost wsrr.company.com —wsrrPort 9443 —wsrrSubscription
    C:\wsrr_subscription.xml —wsrrUsername admin —wsrrPassword adminpassword
    -useProxy true —proxyHost proxy.company.com —proxyPort 80 —proxyUsername proxy1
    —proxyPassword proxypassword
```

- On Linux and UNIX systems:

```
./kd4WSRRSubscriber.sh —wsrrHost wsrr.company.com —wsrrPort 9443 —wsrrSubscription
    C:\wsrr_subscription.xml —wsrrUsername admin —wsrrPassword adminpassword
    -useProxy true —proxyHost proxy.company.com —proxyPort 80 —proxyUsername proxy1
    —proxyPassword proxypassword
```

If the proxy server does not require authentication, do not use the —proxyUsername and the —proxyPassword options.

Example of the output from the deployment script:

```
C:\ITM\CNPS\Products\KD4\latest\bin>kd4WSRRSubscriber.bat -wsrrHost server.company.com
      -wsrrPort 9444 -wsrrUsername wasadmin -wsrrPassword wasadmin
      -wsrrSubscription C:\work\wsrr\wsrr_subscription.xml
KD4DM0127I Establishing a connection to server.company.com:9444...
KD4DM0128I Performing the SSL handshake...

KD4DM0131I The server sent 2 certificate(s).

KD4DM0127I Establishing a connection to server.company.com:9444...
KD4DM0128I Performing the SSL handshake...

KD4DM0129I The certificate is trusted.
KD4DM0125I The subscription has been successfully created. Server response:

<properties>
  <property name="bsrURI" value="5c17ee5c-d486-4629.9bc4.2a97192ac402"/>
```

```
</properties>
```

```
KD4DM0132I The WSRR subscription tool has finished.
```

Important: If you modify the subscription definition file, you must delete the
subscription using the WSRR user interface and then run the script again. For
details, see the WSRR information center located at URLhttp://
publib.boulder.ibm.com/infocenter/sr/v7r5/topic/com.ibm.sr.doc/
twsr_mansrvce_governanceuserguide30.html.

Chapter 6. Synchronizing WSRR and ITCAM for SOA

After configuring or reconfiguring the WSRR subscription for ITCAM for SOA, run the synchronization script. This script ensures that WSRR sends all current SLD information to ITCAM for SOA, and that ITCAM for SOA creates up-to-date situations. After running this script, WSRR sends any future changes automatically, and ITCAM for SOA processes them.

About this task

Complete the following steps to run the synchronization script.

Procedure

1. On the ITCAM for SOA host, change to the *KD4_DIR*/bin directory.
2. Run the following command:
   - On Windows systems: kd4WSRRITMSynchronization.bat *arguments*
   - On Linux and UNIX systems: ./kd4WSRRITMSynchronization.sh *arguments*

   Use the following arguments.

Table 4. Command-line arguments for the synchronization script

Command-line argument	Description
-sdmsHost *hostname*	The name of the Tivoli Enterprise Portal Server host.
-sdmsPort *port*	The Tivoli Enterprise Portal Server HTTP transport port number. The default HTTP transport port number is 15210.
-sdmsUsername *username*	The IBM Tivoli Monitoring user name. The user must be an IBM Tivoli Monitoring administrative user. You can use the user name that has an alias in WSRR (see Creating an authentication alias for an IBM Tivoli Monitoring user″ on page 6).
-sdmsPassword *password*	The IBM Tivoli Monitoring password for the user.

Table 4. Command-line arguments for the synchronization script (continued)

Command-line argument	Description
-wsrrInstances *instances*	The names of the WSRR instances to be synchronized, specified in the format [*wsrr_instance_1*,*wsrr_instance_2*]. (optional) When -wsrrInstances is used, the name given as arguments are the WSRR Instance names (as defined in the WSRR SDMS configuration file) and not the host name of the WSRR Instances. The WSRR instance name must match the same string value that is used by the NAME attribute of the <wsrr_instance> tag under <wsrr_instances> in WSRR SDMS configuration file (see WSRR instances˝ on page 41). **Note:** If the -wsrrInstances argument is not specified, ITCAM for SOA synchronizes with all of the instances of WSRR that are configured.

To determine the SDMS port number, see the HTTP transport port parameter in the following file on the Tivoli Enterprise Portal Server host:

- On Windows systems, *ITM_home*\CNPSJ\profiles\ITMProfile\logs\ AboutThisProfile.txt
- On Linux and UNIX systems, *ITM_home*/*architecture*/iw/profiles/ ITMProfile/logs/AboutThisProfile.txt

Examples

The ITCAM for SOA situations can be synchronized with all WSRR instances or a subset of WSRR instances. On a Windows system, the following command synchronizes all of the ITCAM for SOA situations with the subscribable SLDs of all WSRR instances.

```
kd4WSRRITMSynchronization.bat –sdmsHost teps.company.com –sdmsPort 15210
 –sdmsUsername admin –sdmsPassword adminpassword
```

The Tivoli Enterprise Portal server in this example is on the teps.company.com host on port 15210 with the specified user name and password.

The following command on a Linux or UNIX system has the same effect:

```
./kd4WSRRITMSynchronization.sh –sdmsHost teps.company.com –sdmsPort 15210
–sdmsUsername admin –sdmsPassword adminpassword
```

On a Windows system, the following command synchronizes all of the ITCAM for SOA situations with the subscribable SLDs of the WSRR instances specified using the -WSRRInstances argument:

```
kd4WSRRITMSynchronization.bat –sdmsHost teps.company.com –sdmsPort 15210
–sdmsUsername admin –sdmsPassword adminpassword -wsrrInstances [wsrr_instance_1,wsrr_instance_2]
```

The WSRR instances in this example are defined in the WSRR SDMS configuration file as wsrr_instance_1 and wsrr_instance_2.

The following command on a Linux or UNIX system has the same effect:

```
./kd4WSRRITMSynchronization.sh —sdmsHost teps.company.com —sdmsPort 15210
—sdmsUsername admin —sdmsPassword adminpassword -wsrrInstances [wsrr_instance_1,wsrr_instance_2]
```

Important: The synchronization script relies on the process rule for the RESYNC
event. This rule is present in the default WSRR SDMS configuration file. For
information about using the default file, see Creating the subscription definition
file" on page 19. If you customize the file, make sure that the rule is still in place.
Otherwise the synchronization script does not work.

Important: If any SLD contains invalid entries, for example, offline service
endpoints, SDMS can not create or update situations for the SLDs, and the
synchronization reports an exception. However, all SLDs that have valid entries are
still processed correctly.

Chapter 7. Customizing the integration process

If you use the default settings to configure WSRR integration with ITCAM for SOA, ITCAM for SOA subscribes to all SLD information in WSRR. The SOA Domain Management Server (SDMS) creates and starts situations for active SLDs and remove situations for SLDs that become inactive. You can customize this process using the WSRR SDMS configuration file.

To use the default settings when you configure WSRR integration with ITCAM for SOA, see Creating the WSRR SDMS configuration file″ on page 15 and Creating the subscription definition file″ on page 19.

Important: If the governance enablement profile for WSRR is customized, you must use the same details to customize the SDMS configuration for WSRR integration. The WSRR specialist who performs the customization must provide the URIs and other detailed information for use in the SDMS configuration.

Most settings in the configuration for WSRR 7.5 and 8.0 are the same, but there are additional settings for WSRR 8.0.

Default process overview

The default process, defined in the WSRR SDMS configuration file template and the subscription definition file template, provides a setup that monitors compliance with all of the SLDs that are defined in WSRR.

Default subscription definition

The subscription definition in the template creates a single subscription that covers the following WSRR event types:
- update
- create
- delete
- transition
- remove governance

Default process rules

The WSRR SDMS configuration file template defines process rules that govern creating, updating, starting, stopping, and deleting of ITCAM for SOA situations according to the progress of SLDs, policies, and services in the WSRR lifecycle.

This lifecycle is described in the WSRR Governance Enablement Profile. The process rules in the default WSRR SDMS configuration file template use the lifecycle that is defined in the default Governance Enablement Profile.

All of the situations have the same standard parameters, defined in the WSRR SDMS configuration file (see Situation parameters″ on page 34). The URI, policy formula, and policy advice are copied from the policy that is attached to the SLD into the situation.

The following rules apply to SLD changes, only if the SLD includes governance profile extensions or a governance enablement model:

- When an SLD transitions to *Approve Specification*, SDMS creates and starts a situation based on the SLD. This rule applies if the SLD meets the following conditions:
  - A monitoring policy is attached to the SLD.
  - The SLD defines service endpoints that are online.
  - The SLD applies to services in the operation environment (Production, Staging, Test, or Development).
  - All the service endpoints that are defined are in the "online" governance state.
- When an SLD is deleted or it transitions to *Deprecate* or to *Remove Governance*, SDMS deletes the situation based on the SLD.
- When an SLD transitions to *Supercede*, SDMS stops a situation based on the SLD.
- When an SLD is updated, SDMS creates and starts a situation based on the SLD if such a situation does not exist. If the situation exists, SDMS updates it. This rule applies if the SLD meets the following conditions:
  - The SLD is subscribable.
  - A monitoring policy is attached to the SLD.
  - The SLD defines service endpoints that are online.
  - The SLD applies to services in the operation environment (Production, Staging, Test, or Development).
  - All the service endpoints that are defined are in the "online" governance state.
- When a policy is attached to an SLD, SDMS creates a situation based on the policy. This rule applies if the SLD meets the following conditions:
  - The SLD is subscribable.
  - A monitoring policy is attached to the SLD.
  - The SLD defines service endpoints that are online.
  - The SLD applies to services in the operation environment (Production, Staging, Test, or Development).
  - All the service endpoints defined are in the "online" governance state.
- When a policy is detached from an SLD, when governance is removed from an attached policy, or when a policy attached to an SLD transitions to *Retire from Use* or *Revoke*, SDMS deletes the situation based on the policy.
- On transition of an attached policy to *Approve for Production*, SDMS creates and starts a situation based on the policy. This rule applies if the SLD meets the following conditions:
  - The SLD is subscribable.
  - A monitoring policy is attached to the SLD.
  - The SLD defines service endpoints that are online.
  - The SLD applies to services in the operation environment (Production, Staging, Test, or Development).
- When a policy attached to an SLD is updated, SDMS creates and starts a situation based on the policy if such a situation does not exist. If the situation exists, SDMS updates it. This rule applies if the SLD meets the following conditions:
  - The SLD is subscribable.
  - A monitoring policy is attached to the SLD.
  - The SLD defines service endpoints that are online.

- The SLD applies to services in the operation environment (Production, Staging, Test, or Development).
- All the service endpoints defined are in the "online" governance state.
- If any service operations are available for the SLD, they must be in the "operational" governance state.
- For WSRR 8.0, when a policy attached to an SLD transitions to *Approve Specification*, SDMS creates and starts a situation based on the policy if such a situation does not exist. This rule applies if the SLD meets the following conditions:
  - The SLD is subscribable.
  - A monitoring policy is attached to the SLD.
  - The SLD defines service endpoints that are online.
  - The SLD applies to services in the operation environment (Production, Staging, Test, or Development).
  - All the service endpoints defined are in the "online" governance state.
  - If any service operations are available for the SLD, they must be in the "operational" governance state.
- For WSRR 8.0, when a policy attached to an SLD transitions to *Deprecate*, SDMS deletes the situation based on the policy.
- For WSRR 8.0, when a policy attached to an SLD is redefined (the definition of the policy is being "redefined", and the policy is no longer in an acceptable state based on the processing rules), SDMS deletes the situation based on the policy. If the policy is changed and moved back into an acceptable state, a new situation is created according to other process rules.

The following rules apply to service endpoint changes in an SLD, only if the service endpoint refers to a SOAP, MQ, or Extension service, and the SLD is subscribable:

- When a service endpoint transitions to *Approve for Use*, SDMS creates and starts a situation based on the SLD policy expression for this service endpoint. This rule applies if the SLD meets the following conditions:
  - A monitoring policy is attached to the SLD.
  - If any other endpoints or available operations exist for this SLD, they must apply to services in the operation environment (Production, Staging, Test, or Development). All endpoints must be in the "online" governance state.
- When a service endpoint transitions to *Revoke for Use*, when a service endpoint is deleted, or if governance is removed from a service endpoint, SDMS deletes the situation based on the SLD policy expression for this service endpoint.
- When a service endpoint is updated, SDMS creates and starts a situation based on the SLD policy expression for this service endpoint if it does not exist, or updates the situation if it exists. This rule applies if the SLD meets the following conditions:
  - A monitoring policy is attached to the SLD.
  - If any other endpoints or available operations exist for this SLD, they must apply to services in the operation environment (Production, Staging, Test, or Development). All endpoints must be in the "online" governance state.

When a service endpoint in an SLD changes, SDMS creates and starts a situation based on the SLD if such a situation does not exist. If the situation exists, SDMS updates it. This rule applies if the SLD meets the following conditions:

- The SLD is subscribable.

- A monitoring policy is attached to the SLD.
- The SLD defines service endpoints that are online.
- If the SLD defines service operations, all of them must be in the "operational" governance state.

When a service operation is deleted or it transitions to a non-operational state, or if governance is removed from a service operation, SDMS updates or deletes the situation based on the SLD policy expression of this service operation.

When a service endpoint transitions to a operational˝ governance state, SDMS creates or updates a situation based on an SLD that refers to the service operation that has transitioned. This rule applies if the SLD meets the following conditions:
- The SLD is subscribable.
- A monitoring policy is attached to the SLD.
- The SLD defines service endpoints that are online.
- If the SLD defines service operations, all of them must be in the "operational" governance state.

Also, if the synchronization tool sends a resynchronization request (see Chapter 6, Synchronizing WSRR and ITCAM for SOA," on page 25), SDMS resynchronizes and starts all situations that must be active according to the rules in this section.

For the details of the rules, see Customizing situation management" on page 55.

Important: If any service endpoints or service operations defined for an SLD, they must all be valid and online at the time of a transaction. If any of them are offline or invalid, SDMS does not create or update any situations for the transaction. (It still deletes situations when required). This behavior is mandatory for SDMS; you cannot change it using the configuration file.

Important: If WSRR uses a governance profile other than the default profile, you might have to update the WSRR SDMS configuration file for ITCAM for SOA to integrate with WSRR correctly.

Configuration syntax reference

The top level tag of the WSRR SDMS configuration file is <sdms-config>.

Under the <sdms-config> tag, the following tags can be found:
- The <itm-instance> tag defines the configuration for the entire Tivoli Monitoring instance.
- The <aliases> tag contains definitions of aliases for WSRR URIs that are applied to various fields in the configuration. Each definition is an <alias> tag within this tag.
- The <situation-configurations> tag, containing a definition of parameters for situations that SDMS is to create for monitoring services according to WSRR policies.
- The <wsrr-instances> tag defines the configuration for WSRR instances with which SDMS communicates. All other configuration is done for every instance separately, under the <wsrr-instance> tag within this tag.

Under the <wsrr-instance> tag for every WSRR instance, the following tags can be found:

- The <classification-filter-refs> tag defines the filters that SDMS applies to a message from WSRR. The filters are referenced in process rules and determine whether the process rule applies to a particular message.
- The <wsrr-model> tag defines custom properties related to the WSRR governance enablement profile.
- The <subscriptions> tag contains definitions of subscriptions to WSRR events. A subscription is defined by a <subscription> tag; usually there is one subscription for a WSRR instance.

Within the <subscription> tag, the <process-rules> tag contains the process rules that determine the processing of WSRR messages. The process rules define the logic of SDMS integration with WSRR.

Important: After modifying the WSRR SDMS configuration file, you must deploy it again. See Chapter 4, Creating and deploying the WSRR SDMS configuration file," on page 15.

Tivoli Monitoring instance

The Tivoli Monitoring instance definition contains the host name and credentials for the Tivoli Enterprise Portal server.

The configuration file must contain one Tivoli Monitoring instance definition in the <itm-instance> tag. The <itm-instance>tag is within the <sdms-config> tag.

Set the following attributes in the <itm-instance> tag:

Table 5. Attributes of the <itm-instance> tag

Attribute name	Value
host	The host name or IP address of the Tivoli Enterprise Portal Server (defaults to localhost).
port	Either the configured HTTP transport port or the KFW_EWAS_PORT number of the Tivoli Enterprise Portal Server. The value defaults to 15200, which is the default KFW_EWAS_PORT number. You can optionally change it to the HTTP transport port number. To determine the HTTP transport port number, see the HTTP Transport Port attribute specified in the following file on the Tivoli Enterprise Portal Server host: • On Windows systems, *ITM_home*\CNPSJ\profiles\ITMProfile\ logs\AboutThisProfile.txt • On Linux and UNIX systems, *ITM_home*/*architecture*/iw/profiles/ ITMProfile/logs/AboutThisProfile.txt

Set the following attributes in the <itm-user> tag:

Table 6. Attributes of the <itm-user> tag

Attribute name	Value
username	The username of the Tivoli Monitoring administrative user that also has an alias in WSRR (see Creating an authentication alias for an IBM Tivoli Monitoring user″ on page 6).
password	The password for this user.

Example

```
<itm-instance host="localhost" port="15200">
    <itm-users>
        <itm-user password="password" username="userid"/>
    </itm-users>
</itm-instance>
```

Situation parameters

The situation parameters definition contains the parameters that SDMS sets for every ITCAM for SOA situation that it creates automatically.

A situations parameters definition is contained in the <situation-configurations> tag under the <sdms-config> tag in the WSRR SDMS configuration file. Within the <situation-configurations> tag, a <situation-configuration> tag contains the definition. The name attribute of the <situation-configuration> tag contains the name for this definition. If multiple situation parameter definitions exist, the name must be different for every definition. You can edit the existing definition in the WSRR SDMS configuration file, replacing the values as necessary. At least one situation parameters definition must exist for each WSRR instance. You can create multiple situation parameter definitions if you configure more than one WSRR instance (see WSRR instances″ on page 41).

You can also create a situation parameters definition under the <process-rule> element of each process rule. The situation parameters definition of the process rule takes precedence over the situation parameters definition of the WSRR instance. When the <situation-configuration> tag is added to a process rule, the situation parameters definition applies on the next WSRR notification that triggers the process rule.

Important: The <situation-configuration> tag under a process rule does not contain the name attribute. Because only one situation parameters definition can be specified per process rule, you do not need to differentiate between <situation-configuration> tags.

Under the <situation-configuration> tag, you can set the situation parameters using <property> tags. The "name" attribute contains the parameter name, and the "value" attribute sets the parameter value. You can set the following situation parameters:

Table 7. Situation parameters

Property name	Situation parameter
situation.longname.format.sld	The long name of the situation. You can specify the long name using macros in the format `ibm_${SIT_ID}_${SIT_TABLE}_${SIT_STATUS}_${SLD_NAME}_${SLD_BSRURI}_${POLICY_NAME}_${POLICY_BSRURI}`. Table 8 on page 36 presents a definition of each macro. Macros are substituted with valid data when a situation is created or updated. For example: `${SLD_NAME}-${POLICY_NAME}`. The following rules apply: • If the `situation.longname.format.sld` property is omitted from the situation configuration or if the property is provided but is empty, a default value of `cust_${SIT_TABLE}_${SIT_STATUS}_soa_${SIT_ID}` is used. • The maximum length of the long name of a situation in ITM is 256 characters. If the long name created has more than 256 characters, it is truncated. • The value of the `situation.longname.format.sld` property is treated as text, apart from the macro name. For example, if the value of a macro contains the symbols \$, {, or }, these symbols are treated as text. • If the situation status is not included in the situation action, and if the macro `${SIT_STATUS}` is specified in the `situation.longname.format.sld` property, the value is set to the *unkn*. • If the combination of macros specified does not uniquely identify the situation, the Manage Situations view may not display the complete list of situations. However, all situations are displayed in the Situation Editor. **Important:** To uniquely identify a situation, include the macro ${SIT_ID} in the `situation.longname.format.sld` property.
situation.description	A description of the situation. You can specify the description using macros in the format `SLD:${SLD_NAME}Policy:${POLICY_NAME}`. Table 9 on page 37 presents a definition of each macro. Macros are substituted with valid data when a situation is created or updated. The maximum length of a description in ITM is 64 characters. If the description created has more than 64 characters, it is truncated
situation.distribution	The distribution string, for example `*SERVICE_MANAGEMENT_AGENT_ENVIR`
situation.sampling.interval	The sampling interval (in seconds)
situation.run.at.startup	Whether the situation is started when ITCAM for SOA starts (`true` or `false`) **Note:** If this parameter is used within a process rule definition, it takes precedence over the value of the startOn attribute of the <process-rule> tag.

Table 7. Situation parameters (continued)

Property name	Situation parameter
situation.tec.forwarding	An indication of whether events are fired when the situation triggers. Valid values are `true` or `false`. The default value is true. The `situation.tec.forwarding` property must be set to true for event forwarding to be enabled on the situation in ITM. The Tivoli Event Integration Framework (EIF) must also be enabled.
situation.tec.destination	If forwarding is enabled, list event destination IDs separated by commas. The `situation.tec.destination` property must contain valid event destination IDs for event forwarding to be enabled on the situation in ITM. For the description of an event destination ID, see IBM Tivoli Monitoring documentation at http://publib.boulder.ibm.com/infocenter/tivihelp/v15r1/index.jsp?topic=/com.ibm.itm.doc_6.2.2fp2/welcome.htm.
situation.takeaction.when	Valid values are `first item` or `each item`. This property requires an action to be defined in the monitoring policy for this to apply when a situation is triggered.
situation.takeaction.where	Valid values are `agent` or `TEMS`. This property requires an action to be defined in the monitoring policy for this to apply when a situation is triggered.
situation.takeaction.eachinterval	Whether any action configured for this situation must be repeated every sampling interval while the situation applies (`true` or `false`). This property requires an action to be defined in the monitoring policy for this to apply when a situation is triggered.
situation.until.ttl.format	The time format of the value of the Until interval used in each situation. The time format is specified as `ddd:hh:mm:ss`, where: **ddd** number of days in the interval **hh** number of hours in the interval **mm** number of minutes in the interval **ss** number of seconds in the interval The value of the Until interval is derived from the value of the Until property specified in the WS-Monitoring Policy in WSRR.

You can define the `situation.longname.format.sld` property using the following macros:

Table 8. Macros used in the `situation.longname.format.sld` property

String	Description
${SIT_ID}	Situation identifier.

Table 8. Macros used in the `situation.longname.format.sld` property (continued)

String	Description
${SIT_TABLE}	Abbreviated name of the table in the monitoring policy attached to the SLD. Valid values are flt, siri, si, mat, or ei where: • flt is Fault Log • siri is Services Inventory ReqId 610 • si is Services Inventory 610 • mat is Message Arrival Threshold Table 610 • ei is Endpoint Inventory
${SIT_STATUS}	Abbreviated name of the situation status in the ITM action section of the monitoring policy attached to the SLD. Valid values are falt, crit, minr, warn, hmls, or info, where: • falt is fatal • crit is critical • minr is minor • warn is warning • hmls is harmless • info is informational If no status is specified, then an abbreviation of *unkn* is used to represent a value of unknown.
${SLD_NAME}	Name of the SLD in WSRR.
${SLD_BSRURI}	The bsrUri of the SLD in WSRR.
${POLICY_NAME}	The name of the monitoring policy instance in WSRR.
${POLICY_BSRURI}	The bsrUri of the monitoring policy instance in WSRR.

You can define the `situation.description` property using the following macros:

Table 9. Macros used in the `description` property

String	Description
${SLD_NAME}	Name of the SLD in WSRR.
${POLICY_NAME}	Name of the monitoring policy instance in WSRR.

WSRR Instance Example

```
<situation-configurations>
     <situation-configuration name="default">
       <property name="situation.longname.format.sld"
   value="ibm_${SLD_NAME}_${POLICY_NAME}"/>
    <property name="situation.description"
       value="SLD:${SLD_NAME}Policy:${POLICY_NAME}"/>
        <property name="situation.distribution"
      value="*SERVICES_MANAGEMENT_AGENT_ENVIR"/>
        <property name="situation.sampling.interval" value="300"/>
        <property name="situation.run.at.startup" value="true"/>
        <property name="situation.tec.forwarding" value="false"/>
        <property name="situation.tec.destination" value="nil"/>
        <property name="situation.takeaction.when" value="first item"/>
        <property name="situation.takeaction.where" value="agent"/>
        <property name="situation.takeaction.eachinterval" value="false"/>
```

```
                    <property name="situation.takeaction.where" value="agent"/>
                    <property name="situation.until.ttl.format" value="ddd:hh:mm:ss"/>
          </situation-configuration>
          </situation-configurations>
```

Process Rule Example

```
<process-rule event="TRANSITION" operation="create" represents="SLD_Relation_Transition"
 resourceToSubscribedRelationship="sameObject" startOn="none"
 transition="alias_v6r3.ld.approve.for.use">
 <situation-configuration>
  <property name="situation.run.at.startup" value="false"/>
 </situation-configuration>
 <rule-primary-types>

  <primary-types resourcePrimaryType="alias_v6r3.sm.soap.service.endpoint"
  subscribedPrimaryType="alias_v6r3.sm.soap.service.endpoint"/>

  <primary-types resourcePrimaryType="alias_v6r3.sm.mq.service.endpoint"
  subscribedPrimaryType="alias_v6r3.sm.mq.service.endpoint"/>

  <primary-types resourcePrimaryType="alias_v6r3.sm.extension.service.endpoint"
  subscribedPri maryType="alias_v6r3.sm.extension.service.endpoint"/>

 </rule-primary-types>

 <classification-filters>
  <ref-classification-filter name="sld-subscribable-govn-cf"/>
  <ref-classification-filter name="policy-expression-govn-cf"/>
 </classification-filters>

 <relationship-filters>
  <relationship-filter appliesTo="ServiceLevelEntity" name="gep63_availableEndpoints"
  ordinality="1">
   <ref-classification-filter name="service-endpoint-envr-cf"/>
   <ref-classification-filter name="service-endpoint-online-cf"/>
  </relationship-filters>

  <relationship-filter appliesTo="ServiceLevelEntity" name="gep63_availableOperations"
   ordinality="0">
   <ref-classification-filter name="service-operation-envr-cf"/>
   <ref-classification-filter name="service-operation-govn-cf"/>
  </relationship-filter>
 </relationship-filters>
</process-rule>
```

In this example, the `situation.run.at.startup` property is set to false for all
situations created by this process rule.

Automatic start of situations

The value of the situation parameter `situation.run.at.startup` determines
whether situations associated with the WSRR instance are started automatically
when ITCAM for SOA is started. In the following example, situations are started
automatically when situations are created or updated, regardless of the value of
the startOn attribute in the <process-rule> tag of process rules:

```
<situation-configurations>
 <situation-configuration name="default">
  <property name="situation.run.at.startup" value="true"/>
  ...
 </situation-configuration>
</situation-configurations>
```

If you want full control over the running status of situations using process rules, set the parameter situation.run.at.startup to false:

```
<situation-configurations>
 <situation-configuration name="default">
  <property name="situation.run.at.startup" value="false"/>
  ...
 </situation-configuration>
</situation-configurations>
```

Important: After modifying the WSRR SDMS configuration file, you need to deploy it again. See Chapter 4, Creating and deploying the WSRR SDMS configuration file," on page 15.

startOn attribute

When the value of the parameter situation.run.at.startup in the <situation-configuration> tag is set to false, add a startOn attribute to a process rule to start situations automatically once they are created or updated. The startOn attribute is added to the <process-rule> tag in a process rule. You can set the startOn attribute to one of the following values:

Table 10. startOn values

Value	Description
create	Start the situation when the process rule creates the situation.
createOrUpdate	Start the situation when the process rule creates or updates the situation.
update	Start the situation when the process rule updates the situation.
none	The running status of the situation is not changed when the process rule creates or updates the situation.

Important: The startOn attribute is optional. If the startOn attribute is added to a process rule that does not result in a situation being created or updated, the startOn attribute is ignored.

In the following example of a process rule, a situation is created or updated on receiving an event notification from WSRR indicating that a policy has been updated:

```
<process-rule event="UPDATE"
     represents="SLD_Policy_Update"
     operation="createOrUpdate"
     resourceToSubscribedRelationship="attachedPolicy"
     resourceType="PolicyExpression">
...
</process-rule>
```

To specify that a situation is started automatically on create or update of a situation, add the startOn attribute to the <process-rule> tag. In the following example, the process rule specifies that a situation is started automatically when a policy attached to an SLD is updated:

```
<process-rule event="UPDATE"
     represents="SLD_Policy_Update"
     operation="createOrUpdate"
     startOn="update"
```

```
                    resourceToSubscribedRelationship="attachedPolicy"
                    resourceType="PolicyExpression">
...
</process-rule>
```

To modify whether a situation is started automatically when a situation is created or updated, modify the value of the startOn attribute in the <process-rule> tag. In the following example, the process rule specifies that a situation is started automatically when the situation is created by the transition of an entity related to an SLD:

```
<process-rule event="TRANSITION"
    represents="SLD_Relation_Transition"
    operation="createOrUpdate"
    startOn="create"
    resourceToSubscribedRelationship="sameObject"
    transition="alias_v6v3.ld.approve.for.use"?
...
</process-rule>
```

In the following example, the process rule has been modified to specify that the situation is started automatically when the situation is created or updated by the transition of an entity related to the SLD:

```
<process-rule event="TRANSITION"
    represents="SLD_Relation_Transition"
    operation="createOrUpdate"
    startOn="createOrUpdate"
    resourceToSubscribedRelationship="sameObject"
    transition="alias_v6v3.ld.approve.for.use"?
...
</process-rule>
```

After modifying the WSRR SDMS configuration file, you need to deploy it again. See Chapter 4, Creating and deploying the WSRR SDMS configuration file," on page 15.

Aliases

The aliases definition determines the URI aliases applied to various fields within the configuration file.

The <aliases> tag is under the top level <sdms-config> tag.

Within this tag, several <alias> tags define URI aliases. The name attribute contains the alias name, and the value attribute contains the URI.

In any value where an URI is required, you can also use an alias in the following way: alias_*aliasname*. For example, alias_v6r3.ld.

The URIs defined in the existing aliases are from the WSRR 7.5 default governance enablement profile. If WSRR uses a governance profile other than the default profile, you might need to change the existing alias values to reflect the governance profile. You can also add new aliases as required, using the same syntax.

Example

```
<aliases>
  <alias name="v6r3.ld"
 value="http://www.ibm.com/xmlns/prod/serviceregistry/lifecycle/v6r3/LifecycleDefinition"/>
  <alias name="situation.policy.domain"
 value="http://www.ibm.com/xmlns/stdwip/2011/02/ws-monitoring"/>
</aliases>
```

WSRR instances

The WSRR instance definition contains the host name and credentials for connecting to a WSRR server.

WSRR instance definitions are placed within the <wsrr-instances> tag under the top level <sdms-config> tag.

Usually you only need one WSRR instance definition, as an environment usually includes one WSRR instance. However, if you have several WSRR instances, you can define each of them, so that ITCAM for SOA can process SLD information from each of the instances. Also, you can define one instance several times, in order to use different situation configuration parameters (see Situation parameters" on page 34) for events and process rules defined under each of the instance definitions.

Specify a WSRR instance definition in the <wsrr-instance> tag under the <wsrr-instances> tag. Edit the existing definition in `wsrr_sdms_config.xml` file. You can set the following attributes for this tag:

Table 11. WSRR instance definition tag attributes

Attribute	Value
name	The name for this WSRR instance. SDMS uses this name to generate situation names. **Important:** Do not change this name after the configuration has been used and any situations have been created.
host	WSRR host name.
port	WSRR port for HTTP or HTTPS connection.
secure	true for an HTTPS connection, false for an HTTP connection.
username	The WSRR user name.
password	The WSRR user password.
situation-configuration	The name of the situation configuration, which determines the parameters of all automatically created situations. Normally "default". See Situation parameters" on page 34.
version	The version of WSRR. **Restriction:** You must set the version to `7.5` for all of the supported versions of WSRR. For example, if you are integrating with WSRR version 8.0.0.1, set the value to `7.5`.

Table 11. WSRR instance definition tag attributes (continued)

Attribute	Value
instancePrefix	The WSRR instance prefix. When multiple WSRR instances are used in the same WebSphere Application Server cell, one must set a prefix during WSRR configuration (optional).
authRealm	HTTP authentication realm (optional).
useProxy	If set to true, SDMS will use an HTTP proxy to connect to WSRR (optional).
proxyHost	The host name of the HTTP proxy (required if useProxy=true).
proxyPort	The port number of the HTTP proxy (required if useProxy=true).
proxyUsername	The user name for authentication with the HTTP proxy (required if useProxy=true).
proxyPassword	The password for authentication with the HTTP proxy (required if useProxy=true).
proxyAuthRealm	HTTP authentication realm for the proxy (optional).
sslTimeout	Timeout for secure connections (optional).
wsrr-model	The custom properties defined for an WSRR instance. See WSRR Model" on page 47.
locale	The Java™ locale for sending information (for example, dates) to WSRR. If the locale is not specified, the system locale is used (optional).

The tags for defining classification filters and subscriptions are placed under the <wsrr-instance> tag.

Example

```
<wsrr-instance host="wsrr.company.com" password="wsrr_password" port="1980"
        secure="true" situation-configuration="default" username="wsrr_username"
        version="7.5" name="WSRRInstance1">
```

Classification filters

SDMS applies classification filters to determine whether a process rule applies to a given transaction.

Classification filters are placed in the <classification-filter-refs> tag under the <wsrr-instance> tag. A name is defined for every classification filter, and multiple process rules can invoke a filter by its name.

Alternatively, you can define a classification filter inside a process rule. However, in this case, you can not reuse the filter in other process rules.

Defining a classification filter

A classification filter is applied to the entity linked to a transaction. It can either *pass* or *fail*. A process rule is only applied if all the classification filters that it uses pass.

To define a classification filter, use the <classification-filter> tag, as shown in the following example:

```
<classification-filter appliesTo="ServiceEndpoint_Governance"
    filter="alias_v6r3.ld"
    uri="alias_v6r3.ld.online">
  <classification uri="alias_v6r3.sm.mq.service.endpoint"/>
  <classification uri="alias_v6r3.sm.soap.service.endpoint"/>
  <classification uri="alias_v6r3.sm.extended.service.endpoint"/>
</classification-filter>
```

In the <classification-filter> tag, use the following attributes:

Table 12. Classification filter attributes

Attribute	Value
appliesTo	The entity information to which the filter applies. If several classification filters are to apply within the same rule (by AND logic), the appliesTo values in them must be different; see Setting the appliesTo parameter" on page 44.
filter	A partial URI that the entity fields must match, usually related to lifecycle stages. If the URI is not matched, the filter fails. (optional)
uri	A more complete URI that the entity fields must match. If the URI is not matched, the filter fails, but this is logged. For log file locations, see Chapter 9, Setting the tracing level," on page 119. Both `filter` and `uri` are normally used for URIs defining a lifecycle stage; in the log, you will be able to determine between an entity where the lifecycle stage is not defined and one with the wrong lifecycle stage. If a lifecycle stage is not required, use the `uri` attribute only.

If the entity passes the tests in these attributes, SDMS checks it against the URIs defined in the <classification> tags. The filter can have many <classification> tags; if the entity matches the URI in at least one of these tags, the filter passes. If the entity does not match any of the URIs, the filter fails.

To define a classification filter reference, within the <classification-filter-refs> tag, place the <classification-filter-ref> tag. In this tag, the `name` attribute defines the name of the filter. Within the <classification-filter-ref> tag, place the <classification-filter> tag defining the filter, as shown in the following example:

```
<classification-filter-ref name="service-endpoint-online-cf">
  <classification-filter appliesTo="ServiceEndpoint_Governance"
      filter="alias_v6r3.ld"
      uri="alias_v6r3.ld.online">
    <classification uri="alias_v6r3.sm.mq.service.endpoint"/>
    <classification uri="alias_v6r3.sm.soap.service.endpoint"/>
    <classification uri="alias_v6r3.sm.extended.service.endpoint"/>
  </classification-filter>
</classification-filter-ref>
```

Setting the appliesTo parameter

The appliesTo attribute does not have a fixed set of values. By the convention used in the default template, classifications that apply to the service level entity must have a value of `ServiceLevelEntity`, and classifications that apply to the policy must have a value of `PolicyExpression`.

If several classification filters are used within the same rule, the appliesTo attribute determines how they are processed.

If the appliesTo values are different, each filter is processed independently. For example, if the following filters are defined for the same rule:

```
<classification-filter appliesTo="value1" uri="filter_uri1">
  <classification uri=class_uri1>
</classificationb-filter>

<classification-filter appliesTo="value2" uri="filter_uri2">
  <classification uri=class_uri2>
</classificationb-filter>
```

then the transaction entity must include all of the following URIs: filter_uri1, filter_uri2, class_uri1, class_uri2.

If the appliesTo values are the same, then all of the values in the <classification-filter> attributes for each filter are still checked independently. However, if the entity matches at least one URI defined in a <classification> tag of either filter, it passes. For example, if the following filters are defined for the same rule:

```
<classification-filter appliesTo="value" uri="filter_uri1">
  <classification uri=class_uri1>
</classification-filter>

<classification-filter appliesTo="value" uri="filter_uri2">
  <classification uri=class_uri2>
</classification-filter>
```

then the transaction entity must include following URIs: filter_uri1, filter_uri2, and either class_uri1 or class_uri2 (but not necessarily both of them).

Predefined classification filters

The template configuration file defines several classification filters. Do not remove any of these filters as the standard process rules use them. You might have to modify the existing classification filters if you need to change the logic of the process rules. For example, modify the `service-endpoint-envr-cf` and `service-operation-envr-cf` filters to exclude some environments (like Development) from processing.

Table 13. Predefined classification filters

Filter name	Filter meaning
policy-expression-govn-cf	A policy expression which is monitored and governance is applied
service-endpoint-online-cf	A service endpoint that is online and applies to an SOAP, MQ, or Extension service
service-endpoint-offline-cf	A service endpoint that is offline and applies to an SOAP, MQ, or Extension service

Table 13. Predefined classification filters (continued)

Filter name	Filter meaning
service-endpoint-envr-cf	A service endpoint that is in one of the following environments: Production, Staging, Test, Development
service-operation-envr-cf	A service operation that is in one of the following environments: Production, Staging, Test, Development
service-operation-govn-cf	A service operation which is approved and governance is applied
sld-subscribable-govn-cf	An SLD which is subscribable and includes governance profile extensions or a governance enablement model

Modifying classification filters

You can modify classification filters according to your requirements for processing WSRR events.

The following examples of classification filter references reflect the default process:

```
<classification-filter-refs>
          <classification-filter-ref name="policy-expression-govn-cf">
             <classification-filter appliesTo="PolicyExpression"
                uri="alias_situation.policy.domain">
                <classification uri="alias_v6r3.ld.policy.approved"/>
                <classification uri="alias_v6r3.ld.monitor"/>
             </classification-filter>
          </classification-filter-ref>

          <classification-filter-ref name="service-endpoint-online-cf">
             <classification-filter appliesTo="ServiceEndpoint_Governance"
                filter="alias_v6r3.ld"
                uri="alias_v6r3.ld.online">
                <classification uri="alias_v6r3.sm.mq.service.endpoint"/>
                <classification uri="alias_v6r3.sm.soap.service.endpoint"/>
                <classification uri="alias_v6r3.sm.extension.service.endpoint"/>
             </classification-filter>
          </classification-filter-ref>

          <classification-filter-ref name="service-endpoint-offline-cf">
             <classification-filter appliesTo="ServiceEndpoint_Governance"
                filter="alias_v6r3.ld"
                uri="alias_v6r3.ld.offline">
                <classification uri="alias_v6r3.sm.mq.service.endpoint"/>
                <classification uri="alias_v6r3.sm.soap.service.endpoint"/>
                <classification uri="alias_v6r3.sm.extension.service.endpoint"/>
             </classification-filter>
          </classification-filter-ref>

          <classification-filter-ref name="service-endpoint-envr-cf">
             <classification-filter appliesTo="ServiceEndpoint_Environment"
                filter="alias_v6r3.ld"
                uri="alias_v6r3.ld.online">
                <classification uri="alias_v6r1.gp.taxonomy.production"/>
                <classification uri="alias_v6r1.gp.taxonomy.staging"/>
                <classification uri="alias_v6r1.gp.taxonomy.test"/>
                <classification uri="alias_v6r1.gp.taxonomy.development"/>
             </classification-filter>
          </classification-filter-ref>
```

```
                    <classification-filter-ref name="service-operation-envr-cf">
                        <classification-filter appliesTo="ServiceOperation_Environment"
                            uri="alias_v6r3.sm.service.operation">
                            <classification uri="alias_v6r1.gp.taxonomy.production"/>
                            <classification uri="alias_v6r1.gp.taxonomy.staging"/>
                            <classification uri="alias_v6r1.gp.taxonomy.test"/>
                            <classification uri="alias_v6r1.gp.taxonomy.development"/>
                        </classification-filter>
                    </classification-filter-ref>


                    <classification-filter-ref name="service-operation-govn-cf">
                        <classification-filter appliesTo="ServiceOperation_Governance"
                            uri="alias_v6r3.sm.service.operation">
                            <classification uri="alias_v6r3.ld.capability.approved"/>
                            <classification uri="alias_v6r3.ld.operational"/>
                            <classification uri="alias_v6r3.ld.sld.subscribable"/>
                        </classification-filter>
                    </classification-filter-ref>


                    <classification-filter-ref name="sld-subscribable-govn-cf">
                        <classification-filter appliesTo="ServiceLevelEntity"
                            filter="alias_v6r3.ld"
                            uri="alias_v6r3.ld.sld.subscribable">
                            <classification uri="alias_v6r3.gp.extensions.sld"/>
                            <classification uri="alias_v6r3.ge.model.sld"/>
                        </classification-filter>
                    </classification-filter-ref>

                </classification-filter-refs>
```

To modify a <classification-filter-ref> element, add or remove the <classification>
elements within it. For example, the following classification filter means that the
process rule applies to production, staging, test, and development environments:

```
                <classification-filter-ref name="service-endpoint-envr-cf">
                    <classification-filter appliesTo="ServiceEndpoint_Environment"
                        filter="alias_v6r3.ld"
                        uri="alias_v6r3.ld.online">
                        <classification uri="alias_v6r1.gp.taxonomy.production"/>
                        <classification uri="alias_v6r1.gp.taxonomy.staging"/>
                        <classification uri="alias_v6r1.gp.taxonomy.test"/>
                        <classification uri="alias_v6r1.gp.taxonomy.development"/>
                    </classification-filter>
                </classification-filter-ref>
```

If you want the process rule to apply only to production environments, remove the
staging, test, and development classifications from the filter:

```
                <classification-filter-ref name="service-endpoint-envr-cf">
                    <classification-filter appliesTo="ServiceEndpoint_Environment"
                        filter="alias_v6r3.ld"
                        uri="alias_v6r3.ld.online">
                        <classification uri="alias_v6r1.gp.taxonomy.production"/>
                    </classification-filter>
                </classification-filter-ref>
```

You can also remove a filter from a process rule if it is not required. For example,
the following process rule includes the `service-endpoint-envr-cf` filter, which
defines the environments where the process rule applies:

```
<process-rule event="TRANSITION"
                represents="SLD_Policy_Transition"
                startOn="create"
                operation="create"
                resourceToSubscribedRelationship="attachedPolicy"
```

```
                        resourceType="PolicyExpression"
                        transition="alias_v6r3.ld.approve.production">

                        <rule-primary-types>
                            <primary-types subscribedPrimaryType="alias_v6r3.gp.extensions.sld"/>
                            <primary-types subscribedPrimaryType="alias_v6r3.ge.model.sld"/>
                        </rule-primary-types>

                        <classification-filters>
                            <ref-classification-filter name="policy-expression-govn-cf"/>
                            <ref-classification-filter name="sld-subscribable-govn-cf"/>
                        </classification-filters>

                        <relationship-filters>

                            <relationship-filter appliesTo="ServiceLevelEntity"
                                name="gep63_availableEndpoints" ordinality="1">
                                <ref-classification-filter name="service-endpoint-envr-cf"/>
                                <ref-classification-filter name="service-endpoint-online-cf"/>
                            </relationship-filter>

                            <relationship-filter appliesTo="ServiceLevelEntity"
                                name="gep63_availableOperations" ordinality="0">
                                <ref-classification-filter name="service-operation-envr-cf"/>
                                <ref-classification-filter name="service-operation-govn-cf"/>
                            </relationship-filter>

                        </relationship-filters>
                    </process-rule>
```

If you delete the line that is highlighted, `<ref-classification-filter name="service-operation-envr-cf"/>`, the process rule applies in all environments.

WSRR Model

Custom properties related to the governance enablement profile used by a WSRR can be defined for each WSRR instance.

Custom properties are defined in the <model-properties> tag under the <wsrr-model> tag, which is located under the <wsrr-instance> tag. The value of these properties may need to be updated if the WSRR Governance Enablement Profile has been customized.

Under the <model-properties> tag, you can set the custom properties using <property> tags. The "name" attribute sets the property name, and the "value" attribute sets the property value. You can set the following custom properties:

Table 14. Custom properties

Property name	Value
service.endpoint.relation	The name of the service endpoint relationship in the WSRR metadata for a resource. The property refers to all deployed, callable endpoints that realize an SLD and its associated SLAs. This name is defined in the WSRR governance enablement profile; in the default profile, it is gep63_availableEndpoints. **Note:** Prior to ITCAM for SOA version 7.2, the service.endpoint.relation property was defined in the <situation-configuration> tag in the SDMS configuration file. In ITCAM for SOA version 7.2, if the service.endpoint.relation property is not defined as part of the <model-properties> tag, SDMS uses the service.endpoint.relation property in the <situation-configuration> tag, if defined, for backward compatability.
service.operation.relation	The name of the service operation relationship in the WSRR metadata for a resource. The property refers to the operations provided by the services that an SLD supports. This name is defined in the WSRR governance enablement profile; in the default profile, it is gep63_availableOperations. **Note:** Prior to ITCAM for SOA version 7.2, the service.operation.relation property was defined in the <situation-configuration> tag in the SDMS configuration file. In ITCAM for SOA version 7.2, if the service.operation.relation property is not defined as part of the <model-properties> tag, SDMS uses the service.operation.relation property in the <situation-configuration>, if defined, for backward compatability.
sm.se.service.namespace	The name of the property in the WSRR service model metadata that represents the service endpoint namespace.
sm.se.port.name	The name of the property in the WSRR service model metadata that represents the service endpoint port name.
sm.so.interface.namespace	The name of the property in the WSRR service model metadata that represents the service operation interface name.
sm.so.operation.name	The name of the property in the WSRR service model metadata that represents the service operation name.

To define a custom model, create a <model-properties> tag in a <wsrr-model> tag and place it under a <wsrr-instance>tag as shown in the following example:

```
<wsrr-instance host="wsrr.company.com" port="1980" username="wsrr_username"
 password="wsrr_password" situation-configuration="default" secure="true" version="7.5"
 name="WSRRInstance1"
```

```
<wsrr-model>
      <model-properties>
          <property name="service.endpoint.relation" value="gep63_availableEndpoints"/>
          <property name="service.operation.relation" value="gep63_availableOperations"/>
          <property name="sm.se.service.namespace" value="sm63_serviceNamespace"/>
          <property name="sm.se.port.name" value="sm63_portName"/>
          <property name="sm.so.interface.namespace" value="sm63_interfaceNamespace"/>
          <property name="sm.so.operation.name" value="sm63_operationName"/>
      </model-properties>
    </wsrr-model>
</wsrr-instance>
```

Subscriptions

The subscription definition contains the information identifying a WSRR subscription. All process rule definitions are placed under this definition.

Subscription definitions are under the <subscriptions> tag, which is under the <wsrr-instance> tag.

Usually you only need one subscription definition. If you use more than one WSRR subscription for one WSRR instance, create a subscription definition for each of the subscriptions.

A subscription is defined in a <subscription> tag. Edit the existing definition in the WSRR SDMS configuration file. You can set the following attributes for this tag:

Table 15. WSRR instance definition tag attributes

Attribute	Value
correlationID	The subscription correlation ID. This must be the same string as the _correlationID property in the subscription definition file (see Creating the subscription definition file″ on page 19). If several subscriptions are used, the correlation ID must be unique for each of them.
itmuser	The Tivoli Monitoring user name. This must be the administrative user that also has an alias in WSRR (see Creating an authentication alias for an IBM Tivoli Monitoring user″ on page 6) **Important:** On Linux and UNIX systems, the user name must be in upper case.
name	A subscription name.
securityToken	The subscription security token. This must be the same string as the _endPointSecurityToken property in the subscription definition file (see Creating the subscription definition file″ on page 19). If several subscriptions are used, the security token must be unique for each of them.

The <process-rules> tag for defining process rules is placed under the <subscription> tag. If there is more than one subscription, separate process rules are defined for each subscription.

Example

```
<subscription correlationId="CORRELATION_ID" itmuser="ITM_USERNAME"
    name="SUBSCRIPTION_NAME" securityToken="SECURITY_TOKEN">
```

Process rules

Process rules determine the actions that SDMS takes on receiving a notification from WSRR. The notifications inform ITCAM for SOA that a relevant WSRR entity (SLD, policy, service, or operation) has changed.

Process rules are defined under the <process-rules> tag, which is under the <subscription> tag.

To understand how existing process rules work, and to evaluate the impact of any modifications that you have made, you can check the log file (see Chapter 9, Setting the tracing level," on page 119). By default, SDMS logs every transaction received from WSRR, and the way it was processed.

Each process rule is defined within a <process-rule> tag, as shown in the following example:

```
<process-rule event="TRANSITION"
    represents="SLD_Transition"
    startOn="create"
    operation="create"
    resourceToSubscribedRelationship="sameObject"
    transition="alias_v6r3.ld.approve.spec">

 <rule-primary-types>
    <primary-types resourcePrimaryType="alias_v6r3.gp.extensions.sld"
                   subscribedPrimaryType="alias_v6r3.gp.extensions.sld"/>
    <primary-types resourcePrimaryType="alias_v6r3.ge.model.sld"
                   subscribedPrimaryType="alias_v6r3.ge.model.sld"/>
 </rule-primary-types>

 <classification-filters>
    <ref-classification-filter name="policy-expression-govn-cf"/>
 </classification-filters>

 <relationship-filters>

    <relationship-filter appliesTo="ServiceLevelEntity"
       name="gep63_availableEndpoints" ordinality="1">
       <ref-classification-filter name="service-endpoint-envr-cf"/>
       <ref-classification-filter name="service-endpoint-online-cf"/>
    </relationship-filter>

    <relationship-filter appliesTo="ServiceLevelEntity"
       name="gep63_availableOperations" ordinality="0">
       <ref-classification-filter name="service-operation-envr-cf"/>
       <ref-classification-filter name="service-operation-govn-cf"/>
    </relationship-filter>

 </relationship-filters>
</process-rule>
```

Each process rule defines an action. SDMS takes this action if the transaction passes the criteria set in the process rule definition.

Important: If a transaction matches more than one process rule, SDMS applies all actions. This might lead to unnecessary duplication. If you customize process rules, make sure that each rule is defined with enough specific information.

A process rule (<process-rule> tag) contains the following parts:
- Transaction and entity type definition (<rule-primary-types> tag)
- Classification filters (<classification-filters> tag)

- Relationship filters (<relationship-filters> tag)

Action types

To determine the process rule action, use a combination of the `operation` and `startOn` attributes of the <process_rule> tag. The `operation` attribute specifies the situation-related operation to take on receiving an event notification from WSRR. The `startOn` attribute specifies whether to start the situation when a situation is created, updated or both. For information on the mapping of these attributes to the legacy `represents` attribute, see Appendix B, Older version action types," on page 133.

Represents

To specify the type of WSRR event on which to take the action, use the `represents` attribute of the <process-rule> tag. The following values define the WSRR event types:

Table 16. `represents` attribute values

Value	Description
SLD_Transition	Transition of an SLD to a different state
SLD_Update	Modification of an SLD
SLD_Governance	Removal of governance from an SLD
SLD_Relation_Transition	Transition of a relationship for an SLD to a particular lifecycle stage
SLD_Relation_Update	Update of a relationship for an SLD
SLD_Relation_Governance	Update of governance for an SLD
SLD_Relation_Deletion	Deletion of a relationship for an SLD
SLD_Resync	Resynchronization of SLD information
SLD_Policy_Update	Modification of a policy
SLD_Policy_Detach	Detaching a policy from an SLD
SLD_Policy_Attach	Attaching a policy to an SLD
SLD_Policy_Transition	Transition of a policy to a different state
SLD_Policy_Governance	Set of remote governance for a policy
SLD_Delete	Deletion of an SLD

Automatic start types

To specify when to automatically start a situation once it has been created or updated, use the `startOn` attribute of the <process-rule> tag. The following values define when to start the situation:

Table 17. `startOn` attribute values

Value	Description
create	If the process rule creates a situation, start the situation.
createOrUpdate	If the process rule creates or updates the situation, start the situation.
update	If the process rule updates the situation, start the situation.

Table 17. `startOn` attribute values (continued)

Value	Description
none	The running status of the situation is not affected.

Operation types

To specify the type of operation to perform in relation to a situation in ITM, use the `operation` attribute of the <process-rule> tag. The following table provides a list of possible operations and identifies applicable WSRR events for each operation:

Table 18. `Operation` attribute values

Value	Description	WSRR event
Create	Create the situation.	TRANSITION
		ATTACH
CreateOrUpdate	Create or update the situation.	UPDATE
Resync	Resynchronize situations related to WSRR events. Create, update or delete situations as required.	RESYNC
Delete	Delete one or more situations.	TRANSITION
		DELETE
		DETACH
		REMOVE_GOVERNANCE
Start	Start the situation.	TRANSITION
Stop	Stop the situation.	TRANSITION
Update	Update the situation.	DELETE
		UPDATE

Mapping of represents attribute to WSRR event types

The `represents` attribute of the <process-rule> tag maps to `event` attribute in the WSRR event notification:

Table 19. Mapping of WSRR event attribute to the `represents` attribute values

WSRR event attribute values	Represents attribute value
TRANSITION	SLD_Transition
	SLD_Policy_Transition
	SLD_Relation_Transition
REMOVE_GOVERNANCE	SLD_Governance
	SLD_Policy_Governance
	SLD_Relation_Governance
DELETE	SLD_Delete
	SLD_Relation_Delete

Table 19. Mapping of WSRR event attribute to the represents attribute values (continued)

WSRR event attribute values	Represents attribute value
UPDATE	SLD_Update
	SLD_Policy_Update
	SLD_Relation_Update
ATTACH	SLD_Policy_Attach
DETACH	SLD_Policy_Detach
RESYNC	SLD_Resync

In the following WSRR event notification example, the event attribute of the WSRR event notification is set to DELETE.

```
<xml version="1.0" encoding="utf-8"?>
<body:resources
xmlns:body="http://www.ibm.com/xmlns/prod/serviceregistry/HttpPostNotifierPluginMs
gBody">

<body:resource bsrURI="16998716-2b7e-4ec4.a7c0.94b32d94c041"
correlationId="correlation-id1"
securityToken="security-token1"
type="Subscription"
<body:notificationResource event="DELETE" />
<body:resource>
</body:resources>
```

In the corresponding process rule, the value of the event attribute in the <process-rule> tag must also be set to "DELETE" to map to the WSRR notification event:

```
<process-rule event="DELETE"
        represents="SLD_Relation_Delete"
        operation="update"
        resourceToSubscribeRelationship="sameObject"
```

When the WSRR event type matches a process rule, the represents attribute enriches the information of the event attribute by describing the type of operation that took place on the SLD, policy, or service.

Transaction type

The process rule will only apply to a certain WSRR transaction type.

To determine the event type for the transaction, use the event attribute of the <process-rule> tag. The following values define the event types:

Table 20. event attribute values

Value	Event type
TRANSITION	Transition of an SLD, policy, service endpoint, or service operation to a different state
ATTACH	Attaching a policy to an SLD
DETACH	Detaching a policy from an SLD

Table 20. event attribute values (continued)

Value	Event type
RESYNC	Resynchronization of all situations to SLD information. This event is triggered by an utility, see Chapter 6, Synchronizing WSRR and ITCAM for SOA," on page 25.
UPDATE	Modification of an SLD, policy, service endpoint, or service operation
CREATE	Creation of a new SLD, policy, service endpoint, or service operation
DELETE	Deletion of an SLD, policy, service endpoint, or service operation
VALIDATE	Validation of an SLD, policy, service endpoint, or service operation
MAKE_GOVERNANCE	Addition of governance to an SLD, policy, service endpoint, or service operation
REMOVE_GOVERNANCE	Removal of governance from an SLD, policy, service endpoint, or service operation

For the event type TRANSITION, use the `transition` attribute to specify the transition identification URI.

The `resourceToSubscribedRelationship` attribute, if defined, must match the `resourceToSubscribedRelationship` field in the transaction notification.

Entity type

The process rule can only apply if the transaction applies to an entity of a certain type. WSRR supplies the *resource primary type* and *subscribed primary type* for the entity.

In the <rule-primary-types> tag, you can define one or several sets of resource and subscribed primary type values, using the <primary-types> tag. If any pair of values matches the entity, the rule can be applied.

You can use only the `resourcePrimaryType` attribute, only the `subscribedPrimaryType` attribute, or both in the <primary-types> tag. For example:

```
<primary-types resourcePrimaryType="alias_v6r3.gp.extensions.sld">
```

In this example, if the resource primary type matches the URI, the rule can be applied without regard to the subscribed primary type value.

Classification filters

The process rule can only apply if the transaction entity passes one or several classification filters.

In the <classification-filters> tag, you can use classification filters by name using the <ref-classification-filter> tag. Alternatively, you can insert a <classification-filter> tag and place the classification filter definition in the process rule.

For details on classification filter definition and names, see Classification filters" on page 42.

Relationship filters

The process rule can only apply if service endpoints or operations related to the transaction entity exist and pass one or several classification filters.

In the <relationship-filters> tag, you can define one or several relationship filters, using the <relationship-filter> tag with the following attributes:

Table 21. Relationship filter attributes

Attribute	Value
appliesTo	The entity information to which the filter applies. If several relationship filters with the same appliesTo value are used in the same rule, only one of them must pass for the rule may apply; if filters have different appliesTo values, both of them must pass. See Setting the appliesTo parameter" on page 44.
name	The related entities to which this relationship filter applies. You can use the following values: • gep63_availableEndpoints - all the service endpoints related to this entity • gep63_availableOperations - all the service operations related to this entity
ordinality	The minimum number of the related entities that must be present. **Important:** If this number is set to 0 and no related endpoints or operations (as determined by name) are present, the filter will pass without further checks.

Under the <relationship-filter> tag, you can define classification filters that SDMS will apply to the endpoints or operations. You can use classification filters by name using the <ref-classification-filter> tag. Alternatively, you can insert a <classification-filter> tag and place the classification filter definition in the process rule.

For details on classification filter definition and names, see Classification filters" on page 42.

Customizing situation management

By editing the WSRR SDMS configuration file, you can customize the process rules that determine how SDMS processes events from WSRR. You must customize the process rules if you use a custom WSRR governance enablement profile. You can also customize them to modify the process according to the requirements of your environment.

To customize situation management, modify the aliases and process rules in the file.

You can also modify other settings in the WSRR SDMS configuration file, including Tivoli Monitoring instance parameters, default situation parameters, WSRR instance parameters, and subscription information. For a full description of the configuration file syntax, see Configuration syntax reference" on page 32.

Important: After modifying the WSRR SDMS configuration file, you mist deploy it again. See Chapter 4, Creating and deploying the WSRR SDMS configuration file," on page 15.

Aliases

Aliases in the WSRR SDMS configuration file represent full or partial classification URIs, as defined in the WSRR governance enablement profile.

Aliases are defined in the <alias> tags, for example:

```
<alias name="v6r3.ld"
 value="http://www.ibm.com/xmlns/prod/serviceregistry/lifecycle/v6r3/LifecycleDefinition"/>
```

In WSRR, a classification URI can be defined for any object, including SLDs, service endpoints, lifecycle stages, and so on. Process rules can filter events according to the URIs that are specified in the event notification.

In the default WSRR SDMS configuration file template, aliases reflect the URIs that are defined in the default governance enablement profile. The process rules in this template use aliases to filter events.

If you use a governance enablement profile with different URIs, modify the aliases according to this profile. Alternatively, you can modify process rules so that they contain URIs, not aliases.

Aliases are used to simplify the XML file; filters can refer to aliases instead of containing the URIs directly. For a full description of alias syntax, see Aliases" on page 40.

Classification filters

Classification filters determine whether a process rule is applied to a transaction. Some common classification filters are described in the <classification-filter-refs> tag of the WSRR SDMS configuration file. These filters are used in several process rules. You might have to modify the filters if you use a custom governance enablement profile, or if you want to customize the situation management process.

Each classification describes full or partial URIs. To pass a classification filter, any URI in the event notification must match the `filter` attribute (if present) and the `uri` attribute of the <classification-filter> tag, and the `uri` attribute of at least one of the <classification> tags. For a complete description of the classification filter syntax, see Classification filters" on page 42.

SLD has a policy attachment

The following classification filter ensures that the SLD has a policy attachment that has the policy classification URI:

```
<classification-filter-ref name="policy-expression-govn-cf">
    <classification-filter appliesTo="PolicyExpression"
        filter="alias_v6r3.ld"
        uri="alias_v6r3.ld.monitor">
        <classification uri="alias_situation.policy.domain"/>
    </classification-filter>
</classification-filter-ref>
```

SLD has online service endpoints

The following classification filter ensures that the SLD has at least one service
endpoint that is in the online state:

```
<classification-filter-ref name="service-endpoint-online-cf">
    <classification-filter appliesTo="ServiceEndpoint_Governance"
        filter="alias_v6r3.ld"
        uri="alias_v6r3.ld.online">
        <classification uri="alias_v6r3.sm.mq.service.endpoint"/>
        <classification uri="alias_v6r3.sm.soap.service.endpoint"/>
        <classification uri="alias_v6r3.sm.extension.service.endpoint"/>
    </classification-filter>
</classification-filter-ref>
```

SLD has offline service endpoints

The following classification filter ensures that the SLD has at least one service
endpoint that is in the offline state:

```
<classification-filter-ref name="service-endpoint-offline-cf">
    <classification-filter appliesTo="ServiceEndpoint_Governance"
        filter="alias_v6r3.ld"
        uri="alias_v6r3.ld.offline">
        <classification uri="alias_v6r3.sm.mq.service.endpoint"/>
        <classification uri="alias_v6r3.sm.soap.service.endpoint"/>
        <classification uri="alias_v6r3.sm.extension.service.endpoint"/>
    </classification-filter>
</classification-filter-ref>
```

Tip: No process rule in the default WSRR SDMS configuration file template uses
this classification filter. Therefore, you are not required to modify it for a custom
governance enablement profile, unless the configuration file contains customized
process rules that use this filter.

SLD has service endpoints in one of the monitored environments

The following classification filter ensures that the SLD has at least one service
endpoint in one of the monitored environments:

```
<classification-filter-ref name="service-endpoint-envr-cf">
    <classification-filter appliesTo="ServiceEndpoint_Environment"
        filter="alias_v6r3.ld"
        uri="alias_v6r3.ld.online">
        <classification uri="alias_v6r1.gp.taxonomy.production"/>
        <classification uri="alias_v6r1.gp.taxonomy.staging"/>
        <classification uri="alias_v6r1.gp.taxonomy.test"/>
        <classification uri="alias_v6r1.gp.taxonomy.development"/>
    </classification-filter>
</classification-filter-ref>
```

Tip: Modify this classification filter if you do not want to create situations for
SLDs in a certain environment. For example, to avoid creating situations for SLDs
in the development environment, remove the line that references
alias_v6r1.gp.taxonomy.development.

SLD has service operations in one of the monitored environments

The following classification filter ensures that the SLD has at least one service
operation in one of the monitored environments:

```
          <classification-filter-ref name="service-operation-envr-cf">
             <classification-filter appliesTo="ServiceOperation_Environment"
                uri="alias_v6r3.sm.service.operation">
                <classification uri="alias_v6r1.gp.taxonomy.production"/>
                <classification uri="alias_v6r1.gp.taxonomy.staging"/>
                <classification uri="alias_v6r1.gp.taxonomy.test"/>
                <classification uri="alias_v6r1.gp.taxonomy.development"/>
             </classification-filter>
          </classification-filter-ref>
```

Tip: Modify this classification filter if you do not want to create situations for
SLDs in a certain environment. For example, to avoid creating situations for SLDs
in the development environment, remove the line that references
alias_v6r1.gp.taxonomy.development.

SLD has service operations that can be monitored

The following classification filter ensures that the SLD has at least one service
operation that can be monitored according to its lifecycle stage:

```
          <classification-filter-ref name="service-operation-govn-cf">
             <classification-filter appliesTo="ServiceOperation_Governance"
                uri="alias_v6r3.sm.service.operation">
                <classification uri="alias_v6r3.ld.capability.approved"/>
                <classification uri="alias_v6r3.ld.operational"/>
                <classification uri="alias_v6r3.ld.sld.subscribable"/>
              </classification-filter>
          </classification-filter-ref>
```

SLD is subscribable

The following classification filter ensures that the SLD is in a subscribable lifecycle
stage:

```
          <classification-filter-ref name="sld-subscribable-govn-cf">
             <classification-filter appliesTo="ServiceLevelEntity"
                filter="alias_v6r3.ld"
                uri="alias_v6r3.ld.sld.subscribable">
                <classification uri="alias_v6r3.gp.extensions.sld"/>
                <classification uri="alias_v6r3.ge.model.sld"/>
             </classification-filter>
          </classification-filter-ref>
```

SLD 'Approve Specification' Process Rule

The SLD Approve Specification process rule determines the processing of the
WSRR event that is generated when an SLD moves to a subscribable state as part
of the SLD governance lifecycle in WSRR.

When an SLD becomes subscribable, it means that service level agreements can be
established, through the agreed endpoints relationship, to reference this service
level definition. Development can continue against a subscribable service level
definition but no interactions can be undertaken with its endpoints yet. This means
that service level agreements can be approved and enter the inactive state if the
service level definition is subscribable, but cannot be made active until endpoints
become online.

When ITCAM for SOA processes this event, it creates and starts the situations for
any valid monitoring policy attached to the SLD.

For an SLD to reach this point in its lifecycle, a number of governance transitions must be performed in WSRR. Table 22 lists the transitions from a newly created SLD to a subscribable state according to the default WSRR governance enablement profile:

Table 22. The transitions from a newly created SLD to a subscribable state.

WSRR Lifecycle Transition	Transition URI in WSRR event	Event processing in ITCAM for SOA
ProposedScope	http://www.ibm.com/xmlns/prod/serviceregistry/lifecycle/v6r3/LifecycleDefinition#ProposeScope	Ignore
ApprovedScope	http://www.ibm.com/xmlns/prod/serviceregistry/lifecycle/v6r3/LifecycleDefinition#ApproveScope	Ignore
ProposeSpecification	http://www.ibm.com/xmlns/prod/serviceregistry/lifecycle/v6r3/LifecycleDefinition#ProposeSpecification	Ignore
ApproveSpecification	http://www.ibm.com/xmlns/prod/serviceregistry/lifecycle/v6r3/LifecycleDefinition#ApproveSpecification	Process

WSRR Notification Event

When an SLD transitions into the ApproveSpecification governance lifecycle state, WSRR sends an XML notification to ITCAM for SOA, as shown in the following example:

```
<?xml version="1.0" encoding="utf-8"?>
<body:resources xmlns:body="http://www.ibm.com/xmlns/prod/serviceregistry/
HttpPostNotifierPluginMsgBody">
  <body:resource
      bsrURI="65549565-d3ba-4aa8.934f.a025f2a04fb6"
      correlationId="correlation-id1"
      securityToken="security-token1"
      type="Subscription">
    <body:notificationResource  event="TRANSITION"
        resourceBsrURI="29243729-5334-44a7.9cf3.3e234b3ef38a"
        resourceName="MySLD"
        resourcePrimaryType=
"http://www.ibm.com/xmlns/prod/serviceregistry/profile/v6r3/GovernanceProfileExtensions#
ServiceLevelDefinition"
        resourceToSubscribedRelationship="sameObject"
        resourceType="GenericObject"
        subscribedBsrUri="29243729-5334-44a7.9cf3.3e234b3ef38a"
        subscribedName="MySLD"
        subscribedPrimaryType=
"http://www.ibm.com/xmlns/prod/serviceregistry/profile/v6r3/GovernanceProfileExtensions#
ServiceLevelDefinition"
        subscribedType="GenericObject"
transition="http://www.ibm.com/xmlns/prod/serviceregistry/lifecycle/v6r3/
LifecycleDefinition#ApproveSpecification"/>
  </body:resource>
</body:resources>
```

Process Rule Definition

The default WSRR SDMS configuration file template includes the following process rule definition:

```
<!-- =======================================================
SLD 'Approve Specification'
======================================================= -->
<process-rule event="TRANSITION"
 represents="SLD_Transition"
 startOn="create"
 operation="create"
 resourceToSubscribedRelationship="sameObject"
 transition="alias_v6r3.ld.approve.specification">

 <rule-primary-types>
    <primary-types resourcePrimaryType="alias_v6r3.gp.extensions.sld"
                   subscribedPrimaryType="alias_v6r3.gp.extensions.sld"/>
    <primary-types resourcePrimaryType="alias_v6r3.ge.model.sld"
                   subscribedPrimaryType="alias_v6r3.ge.model.sld"/>
 </rule-primary-types>

 <classification-filters>
    <ref-classification-filter name="sld-subscribable-govn-cf"/>
    <ref-classification-filter name="policy-expression-govn-cf"/>
 </classification-filters>

 <relationship-filters>

    <relationship-filter appliesTo="ServiceLevelEntity"
       name="gep63_availableEndpoints" ordinality="1">
       <ref-classification-filter name="service-endpoint-envr-cf"/>
       <ref-classification-filter name="service-endpoint-online-cf"/>
    </relationship-filter>

    <relationship-filter appliesTo="ServiceLevelEntity"
       name="gep63_availableOperations" ordinality="0">
       <ref-classification-filter name="service-operation-envr-cf"/>
       <ref-classification-filter name="service-operation-govn-cf"/>
    </relationship-filter>

 </relationship-filters>
</process-rule>
```

This process rule defines the processing of events that represent the transition of an SLD to an approve specification lifecycle state. If the event matches certain requirements, ITCAM for SOA creates situations for the service level entity.

In the example event, the SLD is identified by the following attribute:
```
subscribedBsrUri="29243729-5334-44a7.9cf3.3e234b3ef38a".
```

The primary types determine that the process rules must be applied to SLDs:
```
<rule-primary-types>
    <primary-types resourcePrimaryType="alias_v6r3.gp.extensions.sld"
                   subscribedPrimaryType="alias_v6r3.gp.extensions.sld"/>
    <primary-types resourcePrimaryType="alias_v6r3.ge.model.sld"
                   subscribedPrimaryType="alias_v6r3.ge.model.sld"/>
</rule-primary-types>
```

The action to take (create and start situations) is determined by the combination of the following two attributes:
```
startOn="create"
operation="create"
```

The following requirements must be met:
- The SLD must be in a subscribable state. This requirement is enforced by the sld-subscribable-govn-cf classification filter reference:

```
<ref-classification-filter name="sld-subscribable-govn-cf"/>
```
- The SLD must have a policy attachment with the policy classification URI. This requirement is enforced by the `policy-expression-govn-cf` classification filter:
```
<ref-classification-filter name="policy-expression-govn-cf"/>
```
- The SLD must have at least one service endpoint associated with it. This requirement is defined by the relationship filter for the `gep63_availableEndpoints` entity of the SLD. This filter also references classification filters to ensure that the service endpoint is online and in one of the monitored environments:
```
<relationship-filter appliesTo="ServiceLevelEntity"
    name="gep63_availableEndpoints" ordinality="1">
  <ref-classification-filter name="service-endpoint-envr-cf"/>
  <ref-classification-filter name="service-endpoint-online-cf"/>
</relationship-filter>
```
- The SLD can have zero or more service operations associated with it. This requirement is defined by the relationship filter for the `gep63_availableOperations` entity of the SLD. This filter references classification filters to ensure that any service operation can be monitored according to its lifecycle stage and is in one of the monitored environments:
```
<relationship-filter appliesTo="ServiceLevelEntity"
    name="gep63_availableOperations" ordinality="0">
  <ref-classification-filter name="service-operation-envr-cf"/>
  <ref-classification-filter name="service-operation-govn-cf"/>
</relationship-filter>
```

Modifying the Process Rule

You might have to modify this process rule if WSRR has a custom governance enablement profile. In this case, ensure that all the URIs in the process rule (including the classification filters that it references) are valid in the custom profile.

Ensure that the URI of the WSRR lifecycle stage that triggers the process rule is correct in the following line:
```
transition="alias_v6r3.ld.approve.specification"
```

If the existing value of the alias does not match the value in the governance enablement profile, change the alias to the new value. Alternatively, use the new value in the process rule instead of the alias.

SLD 'Deprecate' Process Rule

The SLD 'Deprecate' process rule determines the processing of the WSRR event that is generated when an SLD moves to a deprecated state as part of the SLD governance lifecycle in WSRR.

When an SLD becomes deprecated, it means that all existing service level agreements are moved onto the compatible service level definitions, and these endpoints are made inactive. Existing service level agreements must be renegotiated to directly reference the compatible service level definition.

When ITCAM for SOA processes this event, it deletes any situations that were created for this SLD.

An SLD might be deprecated directly, or it might become deprecated after it has been transitioned to a superceded state as part of the SLD lifecycle. Table 23 lists the transition of an SLD to a deprecated state according to the default WSRR governance enablement profile:

Table 23. The transition of an SLD to a deprecated state.

WSRR Lifecycle Transition	Transition URI in WSRR event	Event processing in ITCAM for SOA
Deprecate	http://www.ibm.com/xmlns/prod/serviceregistry/lifecycle/v6r3/LifecycleDefinition#Deprecate	Process

WSRR Notification Event

When an SLD transitions into the 'Deprecate' governance lifecycle, WSRR sends an XML notification to ITCAM for SOA, as shown in the following example:

```
<?xml version="1.0" encoding="utf-8"?>
    <body:resources xmlns:body="http://www.ibm.com/xmlns/prod/serviceregistry/
HttpPostNotifierPluginMsgBody">
        <body:resource bsrURI="65549565-d3ba-4aa8.934f.a025f2a04fb6"
            correlationId="correlation-id1"
            securityToken="security-token1"
            type="Subscription">
        <body:notificationResource event="TRANSITION"
            resourceBsrURI="29243729-5334-44a7.9cf3.3e234b3ef38a"
            resourceName="MySLD"
            resourcePrimaryType=
"http://www.ibm.com/xmlns/prod/serviceregistry/profile/v6r3/GovernanceProfileExtensions#
ServiceLevelDefinition"
            resourceToSubscribedRelationship="sameObject"
            resourceType="GenericObject"
            subscribedBsrUri="29243729-5334-44a7.9cf3.3e234b3ef38a"
            subscribedName="MySLD"
            subscribedPrimaryType=
"http://www.ibm.com/xmlns/prod/serviceregistry/profile/v6r3/GovernanceProfileExtensions#
ServiceLevelDefinition"
          subscribedType="GenericObject"
transition="http://www.ibm.com/xmlns/prod/serviceregistry/lifecycle/v6r3/
LifecycleDefinition#Deprecate"/>
    </body:resource>
</body:resources>
```

Process Rule Definition

The default WSRR SDMS configuration file template includes the following process rule definition:

```
<!-- =======================================================
SLD 'Deprecate'
======================================================= -->
<process-rule event="TRANSITION"
 represents="SLD_Delete"
 operation="delete"
 resourceToSubscribedRelationship="sameObject"
 transition="alias_v6r3.ld.deprecate">
 <rule-primary-types>
    <primary-types resourcePrimaryType="alias_v6r3.gp.extensions.sld"
                   subscribedPrimaryType="alias_v6r3.gp.extensions.sld"/>
    <primary-types resourcePrimaryType="alias_v6r3.ge.model.sld"
                   subscribedPrimaryType="alias_v6r3.ge.model.sld"/>
 </rule-primary-types>
</process-rule>
```

This process rule defines the processing of events that represent the transition of an SLD to a deprecated lifecycle state. ITCAM for SOA deletes situations for the SLD.

In the example event, the SLD is identified by the following attribute:

```
subscribedBsrUri="29243729-5334-44a7.9cf3.3e234b3ef38a"
```

The primary types determine that the process rules must be applied to SLDs:

```
<rule-primary-types>
   <primary-types resourcePrimaryType="alias_v6r3.gp.extensions.sld"
                  subscribedPrimaryType="alias_v6r3.gp.extensions.sld"/>
   <primary-types resourcePrimaryType="alias_v6r3.ge.model.sld"
                  subscribedPrimaryType="alias_v6r3.ge.model.sld"/>
</rule-primary-types>
```

The action to take (delete situations) is determined by the following attribute:

```
operation="delete"
```

Modifying the Process Rule

You might have to modify this process rule if WSRR has a custom governance enablement profile. In this case, ensure that all the URIs in the process rule are valid in the custom profile.

Ensure that the URI of the WSRR lifecycle stage that triggers the process rule is correct in the following line:

```
transition="alias_v6r3.ld.deprecate"
```

If the existing value of the alias does not match the value in the governance enablement profile, change the alias to the new value. Alternatively, use the new value in the process rule instead of the alias.

SLD 'Supercede' Process Rule

The SLD 'Supercede' process rule determines the processing of the WSRR event that is generated when an SLD moves to a superceded state as part of the SLD governance lifecycle in WSRR.

When an SLD becomes superceded, it means that a new compatible service level definition becomes subscribable, with active endpoints, and the provider wants to move consumers and their service level agreements onto this new provided service level definition. No new subscriptions can be made to a service level definition in this state.

When ITCAM for SOA processes this event, it stops the situations that were created for this SLD.

Table 24 lists the transition of an SLD to a superceded state according to the default WSRR governance enablement profile:

Table 24. The transition of an SLD to a superceded state.

WSRR Lifecycle Transition	Transition URI in WSRR event	Event processing in ITCAM for SOA
Supercede	http://www.ibm.com/xmlns/prod/ serviceregistry/lifecycle/v6r3/ LifecycleDefinition#Supercede	Process

WSRR Notification Event

When an SLD transitions into the 'Supercede' governance lifecycle, WSRR sends an XML notification to ITCAM for SOA, as shown in the following example:

```
<?xml version="1.0" encoding="utf-8"?>
<body:resources xmlns:body="http://www.ibm.com/xmlns/prod/serviceregistry/
HttpPostNotifierPluginMsgBody">
    <body:resource bsrURI="65549565-d3ba-4aa8.934f.a025f2a04fb6"
        correlationId="correlation-id1"
        securityToken="security-token1"
        type="Subscription">
    <body:notificationResource event="TRANSITION"
        resourceBsrURI="29243729-5334-44a7.9cf3.3e234b3ef38a"
        resourceName="MySLD"
        resourcePrimaryType=
"http://www.ibm.com/xmlns/prod/serviceregistry/profile/v6r3/GovernanceProfileExtensions#
ServiceLevelDefinition"
        resourceToSubscribedRelationship="sameObject"
        resourceType="GenericObject"
        subscribedBsrUri="29243729-5334-44a7.9cf3.3e234b3ef38a"
        subscribedName="MySLD"
        subscribedPrimaryType=
"http://www.ibm.com/xmlns/prod/serviceregistry/profile/v6r3/GovernanceProfileExtensions#
ServiceLevelDefinition"
        subscribedType="GenericObject"
transition="http://www.ibm.com/xmlns/prod/serviceregistry/lifecycle/v6r3/
LifecycleDefinition#Supercede"/>
  </body:resource>
</body:resources>
```

Process Rule Definition

The default WSRR SDMS configuration file template includes the following process rule definition:

```
<!-- =========================================================
SLD 'Supercede'
========================================================= -->
<process-rule event="TRANSITION"
 represents="SLD_Transition"
 oif yperation="stop"
 resourceToSubscribedRelationship="sameObject"
 transition="alias_v6r3.ld.supersede">
 <rule-primary-types>
    <primary-types resourcePrimaryType="alias_v6r3.gp.extensions.sld"
                   subscribedPrimaryType="alias_v6r3.gp.extensions.sld"/>
    <primary-types resourcePrimaryType="alias_v6r3.ge.model.sld"
                   subscribedPrimaryType="alias_v6r3.ge.model.sld"/>
 </rule-primary-types>
</process-rule>
```

This process rule defines the processing of events that represent a transition of an SLD to a superseded lifecycle state. ITCAM for SOA stops situations for the SLD.

For events that represent a transition of an SLD to a superseded lifecycle state, stop situations for the SLD. In the example event, the SLD is identified by the following attribute:

```
subscribedBsrUri="29243729-5334-44a7.9cf3.3e234b3ef38a"
```

The primary types determine that the process rules must be applied to SLDs:

```
  <rule-primary-types>
    <primary-types resourcePrimaryType="alias_v6r3.gp.extensions.sld"
                   subscribedPrimaryType="alias_v6r3.gp.extensions.sld"/>
    <primary-types resourcePrimaryType="alias_v6r3.ge.model.sld"
                   subscribedPrimaryType="alias_v6r3.ge.model.sld"/>
  </rule-primary-types>
```

The action to take (stop situations) is determined by the following attribute:

```
operation="stop"
```

Modifying the Process Rule

You might have to modify this process rule if WSRR has a custom governance enablement profile. In this case, ensure that all the URIs in the process rule are valid in the custom profile.

Ensure that the URI of the WSRR lifecycle stage triggering the process rule is correct in the following line:

```
transition="alias_v6r3.ld.supersede"
```

If the existing value of the alias does not match the value in the governance enablement profile, change the alias to the new value. Alternatively, use the new value in the process rule instead of the alias.

SLD 'Remove Governance' Process Rule

The SLD 'Remove Governance' process rule determines the processing of the WSRR event that is generated when lifecycle governance is removed from an SLD in WSRR.

When ITCAM for SOA processes this event, it deletes the situations that were created for this SLD.

A WSRR user can remove governance from an SLD directly. There is no transition, as the event is identified as 'REMOVE_GOVERNANCE', and the SLD is both the resource and the subscribed primary type in the event.

Table 25 lists the processing of the WSRR event notification:

Table 25. ITCAM for SOA handling of the removal of governance from an SLD.

WSRR Lifecycle Transition	WSRR event	Event processing in ITCAM for SOA

Remove Governance	`event='REMOVE_GOVERNANCE'`
	`resourcePrimaryType=`
	` <SLD classification URI>`
	`subscribedPrimaryType=`
	` <SLD classification URI>`
		Process

WSRR Notification Event

When governance is removed from an SLD, WSRR sends an XML notification to ITCAM for SOA, as shown in the following example:

```
<?xml version="1.0" encoding="utf-8"?>
<body:resources xmlns:body="http://www.ibm.com/xmlns/prod/serviceregistry/
HttpPostNotifierPluginMsgBody">
  <body:resource bsrURI="65549565-d3ba-4aa8.934f.a025f2a04fb6"
     correlationId="correlation-id1"
```

```
                securityToken="security-token1"
                type="Subscription">
                <body:notificationResource event="REMOVE_GOVERNANCE"
                    resourceBsrURI="29243729-5334-44a7.9cf3.3e234b3ef38a"
                    resourceName="MySLD"
                    resourcePrimaryType=
                        "http://www.ibm.com/xmlns/prod/serviceregistry/profile/v6r3/
GovernanceProfileExtensions#ServiceLevelDefinition"
                    resourceToSubscribedRelationship="sameObject"
                    resourceType="GenericObject"
                    subscribedBsrUri="29243729-5334-44a7.9cf3.3e234b3ef38a"
                    subscribedName="MySLD"
                    subscribedPrimaryType=
                        "http://www.ibm.com/xmlns/prod/serviceregistry/profile/v6r3/
GovernanceProfileExtensions#ServiceLevelDefinition"
                    subscribedType="GenericObject"/>
            </body:resource>
</body:resources>
```

Process Rule Definition

The default WSRR SDMS configuration file template includes the following process
rule definition:

```
<!-- ========================================================
SLD 'Remove Governance'
======================================================== -->
<process-rule event="REMOVE_GOVERNANCE"
 represents="SLD_Governance"
 operation="delete"
 resourceToSubscribedRelationship="sameObject">
 <rule-primary-types>
    <primary-types resourcePrimaryType="alias_v6r3.gp.extensions.sld"
                   subscribedPrimaryType="alias_v6r3.gp.extensions.sld"/>
    <primary-types resourcePrimaryType="alias_v6r3.ge.model.sld"
                   subscribedPrimaryType="alias_v6r3.ge.model.sld"/>
 </rule-primary-types>
</process-rule>
```

This process rule defines the processing of events that represent the removal of
governance from an SLD. ITCAM for SOA deletes situations for the SLD.

In the example event, the SLD is identified by the following attribute:

```
subscribedBsrUri="29243729-5334-44a7.9cf3.3e234b3ef38a"
```

The primary types determine that the process rules must be applied to SLDs:

```
 <rule-primary-types>
    <primary-types resourcePrimaryType="alias_v6r3.gp.extensions.sld"
                   subscribedPrimaryType="alias_v6r3.gp.extensions.sld"/>
    <primary-types resourcePrimaryType="alias_v6r3.ge.model.sld"
                   subscribedPrimaryType="alias_v6r3.ge.model.sld"/>
 </rule-primary-types>
```

The action to take (delete situations) is determined by the following attribute:

```
operation="delete"
```

SLD 'Delete' Process Rule

The SLD 'Delete' process rule determines the processing of the WSRR event that is
generated when an SLD is deleted from WSRR.

When ITCAM for SOA processes this event, it deletes any situations that were
created for this SLD.

The event is identified as 'DELETE'. The SLD is both the resource and the subscribed primary type in the event.

Table 26 lists the handling of the WSRR event notification:

Table 26. ITCAM for SOA handling of the deletion of an SLD.

WSRR action	WSRR event	Event handling in ITCAM for SOA
Delete	event='DELETE' resourcePrimaryType= <SLD classification URI> subscribedPrimaryType= <SLD classification URI>	Process

WSRR Notification Event

When an SLD is deleted, WSRR sends an XML notification to ITCAM for SOA, as shown in the following example:

```
<?xml version="1.0" encoding="utf-8"?>
<body:resources xmlns:body="http://www.ibm.com/xmlns/prod/serviceregistry/
HttpPostNotifierPluginMsgBody">
  <body:resource bsrURI="65549565-d3ba-4aa8.934f.a025f2a04fb6"
    correlationId="correlation-id1"
    securityToken="security-token1"
    type="Subscription">
    <body:notificationResource event="DELETE"
      resourceBsrURI="29243729-5334-44a7.9cf3.3e234b3ef38a"
      resourceName="MySLD"
      resourcePrimaryType=
          "http://www.ibm.com/xmlns/prod/serviceregistry/profile/v6r3/
GovernanceProfileExtensions#ServiceLevelDefinition"
      resourceToSubscribedRelationship="sameObject"
      resourceType="GenericObject"
      subscribedBsrUri="29243729-5334-44a7.9cf3.3e234b3ef38a"
      subscribedName="MySLD"
      subscribedPrimaryType=
          "http://www.ibm.com/xmlns/prod/serviceregistry/profile/v6r3/
GovernanceProfileExtensions#ServiceLevelDefinition"
      subscribedType="GenericObject"/>
  </body:resource>
</body:resources>
```

Process Rule Definition

The default WSRR SDMS configuration file template includes the following process rule definition:

```
<!-- =======================================================
SLD 'Delete'
======================================================= -->
<process-rule event="DELETE"
 represents="SLD_Delete"
 operation="delete"
 resourceToSubscribedRelationship="sameObject">
 <rule-primary-types>
    <primary-types resourcePrimaryType="alias_v6r3.gp.extensions.sld"
                   subscribedPrimaryType="alias_v6r3.gp.extensions.sld"/>
    <primary-types resourcePrimaryType="alias_v6r3.ge.model.sld"
                   subscribedPrimaryType="alias_v6r3.ge.model.sld"/>
 </rule-primary-types>
</process-rule>
```

This process rule defines the processing of events that represent the deletion of an SLD. ITCAM for SOA deletes situations for the SLD.

In the example event, the SLD is identified by the following attribute:

```
subscribedBsrUri="29243729-5334-44a7.9cf3.3e234b3ef38a"
```

The primary types determine that the process rules must be applied to SLDs:

```
<rule-primary-types>
   <primary-types resourcePrimaryType="alias_v6r3.gp.extensions.sld"
                  subscribedPrimaryType="alias_v6r3.gp.extensions.sld"/>
   <primary-types resourcePrimaryType="alias_v6r3.ge.model.sld"
                  subscribedPrimaryType="alias_v6r3.ge.model.sld"/>
</rule-primary-types>
```

The action to take (delete situations) is determined by the following attribute:

```
operation="delete"
```

SLD 'Update' Process Rule

The SLD 'Update' process rule determines the processing of the WSRR event that is generated when an SLD is changed in WSRR. This includes the editing of SLD properties, relationships or classifications.

Overview

When ITCAM for SOA processes this event, it creates situations for the SLD if they do not already exist, or it updates existing situations for the SLD.

The event is identified as 'UPDATE'. The SLD is both the resource and the subscribed primary type in the event.

Table 27 lists the handling of the WSRR event notification:

Table 27. ITCAM for SOA handling of the updating of an SLD.

WSRR action	WSRR event	Event handling in ITCAM for SOA
Edit SLD	event=`UPDATE` resourcePrimaryType= <SLD classification URI> subscribedPrimaryType= <SLD classification URI>	Process

WSRR Notification Event

When an SLD is updated, WSRR sends an XML notification to ITCAM for SOA, as shown in the following example:

```
<?xml version="1.0" encoding="utf-8"?>
<body:resources xmlns:body="http://www.ibm.com/xmlns/prod/serviceregistry/
HttpPostNotifierPluginMsgBody">
  <body:resource bsrURI="65549565-d3ba-4aa8.934f.a025f2a04fb6"
     correlationId="correlation-id1"
     securityToken="security-token1"
     type="Subscription">
     <body:notificationResource event="UPDATE"
        resourceBsrURI="29243729-5334-44a7.9cf3.3e234b3ef38a"
        resourceName="MySLD"
        resourcePrimaryType=
            "http://www.ibm.com/xmlns/prod/serviceregistry/profile/v6r3/
```

```
GovernanceProfileExtensions#ServiceLevelDefinition"
        resourceToSubscribedRelationship="sameObject"
        resourceType="GenericObject"
        subscribedBsrUri="29243729-5334-44a7.9cf3.3e234b3ef38a"
        subscribedName="MySLD"
        subscribedPrimaryType=
            "http://www.ibm.com/xmlns/prod/serviceregistry/profile/v6r3/
GovernanceProfileExtensions#ServiceLevelDefinition"
        subscribedType="GenericObject"/>
  </body:resource>
</body:resources>
```

Process Rule Definition

The default WSRR SDMS configuration file template includes the following process
rule definition:

```
<!-- ========================================================
SLD `Update`
======================================================== -->
<process-rule event="UPDATE"
   represents="SLD_Update"
   startOn="createOrUpdate"
   operation="createOrUpdate"
   resourceToSubscribedRelationship="sameObject">
   <rule-primary-types>
      <primary-types resourcePrimaryType="alias_v6r3.gp.extensions.sld"
                     subscribedPrimaryType="alias_v6r3.gp.extensions.sld"/>
      <primary-types resourcePrimaryType="alias_v6r3.ge.model.sld"
                     subscribedPrimaryType="alias_v6r3.ge.model.sld"/>
   </rule-primary-types>
   <classification-filters>
      <ref-classification-filter name="sld-subscribable-govn-cf"/>
      <ref-classification-filter name="policy-expression-govn-cf"/>
   </classification-filters>
   <relationship-filters>
      <relationship-filter appliesTo="ServiceLevelEntity"
         name="gep63_availableEndpoints" ordinality="1">
         <ref-classification-filter name="service-endpoint-envr-cf"/>
         <ref-classification-filter name="service-endpoint-online-cf"/>
      </relationship-filter>
      <relationship-filter appliesTo="ServiceLevelEntity"
         name="gep63_availableOperations" ordinality="0">
         <ref-classification-filter name="service-operation-envr-cf"/>
         <ref-classification-filter name="service-operation-govn-cf"/>
      </relationship-filter>
   </relationship-filters>
</process-rule>
```

This process rule defines the processing of events that represent an update of an
SLD. If the event matches certain requirements, ITCAM for SOA creates or updates
situations for the service level entity.

In the example event, the SLD is identified by the following attribute:
```
subscribedBsrUri="29243729-5334-44a7.9cf3.3e234b3ef38a".
```

The primary types determine that the process rules must be applied to SLDs:

```
 <rule-primary-types>
    <primary-types resourcePrimaryType="alias_v6r3.gp.extensions.sld"
                   subscribedPrimaryType="alias_v6r3.gp.extensions.sld"/>
    <primary-types resourcePrimaryType="alias_v6r3.ge.model.sld"
                   subscribedPrimaryType="alias_v6r3.ge.model.sld"/>
 </rule-primary-types>
```

The action to take (create or update situations) is determined by the combination of the following two attributes:

```
startOn="createOrUpdate"
operation="createOrUpdate"
```

The following requirements must be met:

- The SLD must be in a subscribable state. This requirement is enforced by the `sld-subscribable-govn-cf` classification filter reference:

  ```
  <ref-classification-filter name="sld-subscribable-govn-cf"/>
  ```

- The SLD must have a policy attachment with the policy classification URI. This requirement is enforced by the `policy-expression-govn-cf` classification filter:

  ```
  <ref-classification-filter name="policy-expression-govn-cf"/>
  ```

- The SLD must have at least one service endpoint associated with it. This requirement is defined by the relationship filter for the `gep63_availableEndpoints` entity of the SLD. This filter also references classification filters to ensure that the service endpoint is online and in one of the monitored environments:

  ```
  <relationship-filter appliesTo="ServiceLevelEntity"
      name="gep63_availableEndpoints" ordinality="1">
    <ref-classification-filter name="service-endpoint-envr-cf"/>
    <ref-classification-filter name="service-endpoint-online-cf"/>
  </relationship-filter>
  ```

- The SLD can have zero or more service operations associated with it. This requirement is defined by the relationship filter for the `gep63_availableOperations` entity of the SLD. This filter references classification filters to ensure that any service operation can be monitored according to its lifecycle stage and is in one of the monitored environments:

  ```
  <relationship-filter appliesTo="ServiceLevelEntity"
      name="gep63_availableOperations" ordinality="0">
    <ref-classification-filter name="service-operation-envr-cf"/>
    <ref-classification-filter name="service-operation-govn-cf"/>
  </relationship-filter>
  ```

SLD Attach Policy Process Rule

The SLD Attach Policy process rule determines the processing of the WSRR event that is generated when a Service Level Monitoring (SLM) policy is attached to an SLD.

Overview

When ITCAM for SOA processes this event, it creates and starts situations for the SLM policy attached to the SLD, if the policy is valid.

The event is identified as ATTACH. The SLD is the subscribed primary type; the resource type is PolicyExpression.

Table 28 on page 71 lists the processing of the WSRR event notification:

Table 28. ITCAM for SOA handling of attaching an SLM policy to an SLD.

WSRR action	WSRR event	Event processing in ITCAM for SOA
Attach Policy	event='ATTACH' resourceToSubscribedRelationship= "attachedPolicy" resourceType= "PolicyExpression" subscribedPrimaryType= <SLD classification URI>	Process

WSRR Notification Event

When a policy is attached to an SLD, WSRR sends an XML event notification to ITCAM for SOA, as shown in the following example:

```
<?xml version="1.0" encoding="utf-8"?>
<body:resources xmlns:body="http://www.ibm.com/xmlns/prod/serviceregistry/
HttpPostNotifierPluginMsgBody">
  <body:resource bsrURI="f1dbd3f1-94a4-44b2.bd6a.639695636a6c"
      correlationId="correlation-id1"
      securityToken="security-token1"
      type="Subscription">
    <body:notificationResource event="ATTACH"
        resourceBsrURI=""
        resourceName=""
        resourceToSubscribedRelationship="attachedPolicy"
        resourceType="PolicyExpression"
        subscribedBsrUri="29243729-5334-44a7.9cf3.3e234b3ef38a"
        subscribedName="MySLD"
        subscribedPrimaryType=
            "http://www.ibm.com/xmlns/prod/serviceregistry/profile/v6r3/
GovernanceProfileExtensions#ServiceLevelDefinition"
        subscribedType="GenericObject">
      <policyUri>urn:Fatal</policyUri>
    </body:notificationResource>
  </body:resource>
</body:resources>
```

Process Rule Definition

The default WSRR SDMS configuration file template includes the following process rule definition:

```
<!-- ========================================================
SLD 'Attach Policy'
======================================================== -->
<process-rule event="ATTACH"
    represents="SLD_Policy_Attach"
    startOn="create"
    operation="create"
    resourceToSubscribedRelationship="attachedPolicy"
    resourceType="PolicyExpression">
    <rule-primary-types>
        <primary-types subscribedPrimaryType="alias_v6r3.gp.extensions.sld"/>
        <primary-types subscribedPrimaryType="alias_v6r3.ge.model.sld"/>
    </rule-primary-types>
    <classification-filters>
        <ref-classification-filter name="sld-subscribable-govn-cf"/>
        <ref-classification-filter name="policy-expression-govn-cf"/>
    </classification-filters>
    <relationship-filters>
        <relationship-filter appliesTo="ServiceLevelEntity"
            name="gep63_availableEndpoints" ordinality="1">
```

```
            <ref-classification-filter name="service-endpoint-envr-cf"/>
            <ref-classification-filter name="service-endpoint-online-cf"/>
        </relationship-filter>
        <relationship-filter appliesTo="ServiceLevelEntity"
            name="gep63_availableOperations" ordinality="0">
            <ref-classification-filter name="service-operation-envr-cf"/>
            <ref-classification-filter name="service-operation-govn-cf"/>
        </relationship-filter>
    </relationship-filters>
</process-rule>
```

This process rule defines the processing of events of the type ATTACH, representing attaching of an SLM policy to a ServiceLevelDefinition. If the event matches certain requirements, ITCAM for SOA creates situations for the policy

In the example event, the SLD is identified by the following attribute:

```
subscribedBsrUri="29243729-5334-44a7.9cf3.3e234b3ef38a".
```

The SLM policy that is attached to the SLD is identified in the WSRR event by the <policyUri> element, as shown in the following example:

```
<policyUri>urn:Fatal</policyUri>
```

The primary types determine that the process rules must be applied to SLDs:

```
    <rule-primary-types>
        <primary-types subscribedPrimaryType="alias_v6r3.gp.extensions.sld"/>
        <primary-types subscribedPrimaryType="alias_v6r3.ge.model.sld"/>
    </rule-primary-types>
```

The following attributes determine that the rule applies to a policy (PolicyExpression) that is attached to the SLD (attachedPolicy):

```
resourceToSubscribedRelationship="attachedPolicy"
resourceType="PolicyExpression">
```

The action to take (create and start situations) is determined by the combination of the following two attributes:

```
startOn="create"
operation="create"
```

The following requirements must be met:
- The SLD must be in a subscribable state. This requirement is enforced by the sld-subscribable-govn-cf classification filter reference:

  ```
  <ref-classification-filter name="sld-subscribable-govn-cf"/>
  ```
- The SLD must have a policy attachment with the policy classification URI. This requirement is enforced by the policy-expression-govn-cf classification filter:

  ```
  <ref-classification-filter name="policy-expression-govn-cf"/>
  ```
- The SLD must have at least one service endpoint associated with it. This requirement is defined by the relationship filter for the gep63_availableEndpoints entity of the SLD. This filter also references classification filters to ensure that the service endpoint is online and in one of the monitored environments:

  ```
  <relationship-filter appliesTo="ServiceLevelEntity"
      name="gep63_availableEndpoints" ordinality="1">
    <ref-classification-filter name="service-endpoint-envr-cf"/>
    <ref-classification-filter name="service-endpoint-online-cf"/>
  </relationship-filter>
  ```
- The SLD can have zero or more service operations associated with it. This requirement is defined by the relationship filter for the

gep63_availableOperations entity of the SLD. This filter references classification filters to ensure that any service operation can be monitored according to its lifecycle stage and is in one of the monitored environments:

```
<relationship-filter appliesTo="ServiceLevelEntity"
      name="gep63_availableOperations" ordinality="0">
   <ref-classification-filter name="service-operation-envr-cf"/>
   <ref-classification-filter name="service-operation-govn-cf"/>
</relationship-filter>
```

SLD 'Detach Policy' Process Rule

The SLD 'Detach Policy' process rule determines the processing of the WSRR event that is generated when a Service Level Monitoring policy is detached from an SLD.

When ITCAM for SOA processes this event, it deletes situations for the SLM policy.

The event is identified as 'DETACH'. The SLD is the subscribed primary type; the resource type is "PolicyExpression".

Table 29 lists the handling of the WSRR event notification:

Table 29. ITCAM for SOA handling of detaching an SLM policy from an SLD.

WSRR action	WSRR event	Event handling in ITCAM for SOA
Detach Policy	event='DETACH' resourceToSubscribedRelationship= "attachedPolicy" resourceType= "PolicyExpression" subscribedPrimaryType= <SLD classification URI>	Process

WSRR Notification Event

When a policy is detached from an SLD, WSRR sends an XML notification to ITCAM for SOA, as shown in the following example:

```
<?xml version="1.0" encoding="utf-8"?>
<body:resources xmlns:body="http://www.ibm.com/xmlns/prod/serviceregistry/
HttpPostNotifierPluginMsgBody">
  <body:resource bsrURI="f1dbd3f1-94a4-44b2.bd6a.639695636a6c"
      correlationId="correlation-id1"
      securityToken="security-token1"
      type="Subscription">
    <body:notificationResource event="DETACH"
        resourceBsrURI=""
        resourceName=""
        resourceToSubscribedRelationship="attachedPolicy"
        resourceType="PolicyExpression"
        subscribedBsrUri="29243729-5334-44a7.9cf3.3e234b3ef38a"
        subscribedName="MySLD"
        subscribedPrimaryType=
            "http://www.ibm.com/xmlns/prod/serviceregistry/profile/v6r3/
GovernanceProfileExtensions#ServiceLevelDefinition"
        subscribedType="GenericObject">
      <policyUri>urn:Fatal</policyUri>
    </body:notificationResource>
  </body:resource>
</body:resources>
```

Process Rule Definition

The default WSRR SDMS configuration file template includes the following process rule definition:

```
<!-- =======================================================
SLD 'Detach Policy'
======================================================= -->
<process-rule event="DETACH"
   represents="SLD_Policy_Detach"
   operation="delete"
   resourceToSubscribedRelationship="attachedPolicy"
   resourceType="PolicyExpression">
   <rule-primary-types>
      <primary-types subscribedPrimaryType="alias_v6r3.gp.extensions.sld"/>
      <primary-types subscribedPrimaryType="alias_v6r3.ge.model.sld"/>
   </rule-primary-types>
</process-rule>
```

This process rule defines the processing of events that represent the detaching of an SLM policy from an SLD. ITCAM for SOA deleted the situations for the policy.

In the example event, the SLD is identified by the following attribute:

```
subscribedBsrUri="29243729-5334-44a7.9cf3.3e234b3ef38a".
```

The SLM policy that is attached to the SLD is identified in the WSRR event by the <policyUri> element, for example:

```
<policyUri>urn:Fatal</policyUri>
```

The primary types determine that the process rules must be applied to SLDs:

```
   <rule-primary-types>
      <primary-types subscribedPrimaryType="alias_v6r3.gp.extensions.sld"/>
      <primary-types subscribedPrimaryType="alias_v6r3.ge.model.sld"/>
   </rule-primary-types>
```

The following attributes determine that the rule applies to a policy (PolicyExpression) that is attached to the SLD (attachedPolicy):

```
resourceToSubscribedRelationship="attachedPolicy"
resourceType="PolicyExpression">
```

The action to take (delete situations) is determined by the following attribute:

```
operation="delete"
```

Policy 'Remove Governance' Process Rule

The Policy 'Remove Governance' process rule determines the processing of the WSRR event that is generated when governance is removed from a Service Level Monitoring policy that is attached to an SLD.

When ITCAM for SOA processes this event, it deletes situations for the SLM policy and SLD.

The event is identified as REMOVE_GOVERNANCE. The SLD is the subscribed primary type; the resource type is PolicyExpression.

Table 30 on page 75 lists the handling of the WSRR event notification:

Table 30. ITCAM for SOA handling of removing governance from an SLD.

WSRR action	WSRR event	Event handling in ITCAM for SOA

Remove Governance	`event='REMOVE_GOVERNANCE'`
	`resourceToSubscribedRelationship=`
	` "attachedPolicy"`
	`resourceType="PolicyExpression"`
	`subscribedPrimaryType=`
	` <SLD classification URI>`
		Process

WSRR Notification Event

When governance is removed from an SLM policy, WSRR sends an XML notification to ITCAM for SOA, as shown in the following example:

```
<?xml version="1.0" encoding="utf-8"?>
<body:resources xmlns:body="http://www.ibm.com/xmlns/prod/serviceregistry/
HttpPostNotifierPluginMsgBody">
  <body:resource bsrURI="f1dbd3f1-94a4-44b2.bd6a.639695636a6c"
    correlationId="correlation-id1"
    securityToken="security-token1"
    type="Subscription">
   <body:notificationResource event="REMOVE_GOVERNANCE"
      resourceBsrURI=""
      resourceName=""
      resourceToSubscribedRelationship="attachedPolicy"
      resourceType="PolicyExpression"
      subscribedBsrUri="29243729-5334-44a7.9cf3.3e234b3ef38a"
      subscribedName="MySLD"
      subscribedPrimaryType=
         "http://www.ibm.com/xmlns/prod/serviceregistry/profile/v6r3/
GovernanceProfileExtensions#ServiceLevelDefinition"
      subscribedType="GenericObject">
     <policyUri>urn:Fatal</policyUri>
   </body:notificationResource>
  </body:resource>
</body:resources>
```

Process Rule Definition

The default WSRR SDMS configuration file template includes the following process rule definition:

```
<!-- =========================================================
Policy 'Remove Governance'
========================================================= -->
<process-rule event="REMOVE_GOVERNANCE"
   represents="SLD_Policy_Governance"
   operation="delete"
   resourceToSubscribedRelationship="attachedPolicy"
   resourceType="PolicyExpression">
   <rule-primary-types>
      <primary-types subscribedPrimaryType="alias_v6r3.gp.extensions.sld"/>
      <primary-types subscribedPrimaryType="alias_v6r3.ge.model.sld"/>
   </rule-primary-types>
</process-rule>
```

This process rule defines the processing of events that represent the removal of governance of an SLM policy from an SLD. ITCAM for SOA deletes the situations that were created for the policy.

In the example event, the SLD is identified by the following attribute:

```
subscribedBsrUri="29243729-5334-44a7.9cf3.3e234b3ef38a".
```

The SLM policy that is attached to the SLD is identified in the WSRR event by the
<policyUri> element, for example:

```
<policyUri>urn:Fatal</policyUri>
```

The primary types determine that the process rules must be applied to SLDs:

```
<rule-primary-types>
    <primary-types subscribedPrimaryType="alias_v6r3.gp.extensions.sld"/>
    <primary-types subscribedPrimaryType="alias_v6r3.ge.model.sld"/>
</rule-primary-types>
```

The following attributes determine that the rule applies to a policy
(PolicyExpression) that is attached to the SLD (attachedPolicy):

```
resourceToSubscribedRelationship="attachedPolicy"
resourceType="PolicyExpression">
```

The action to take (delete situations) is determined by the following attribute:

```
operation="delete"
```

Policy Approve for Production˝ Process Rule

The Policy Approve For Production˝ process rule determines the processing of the
WSRR event that is generated when an Policy moves to a 'Monitor' state as part of
the policy governance lifecycle in WSRR.

When ITCAM for SOA processes this event, it creates and starts situations for the
SLM policy.

The WSRR event is identified as TRANSITION. The SLD is the subscribed primary
type; the resource type is PolicyExpression.

For an SLM policy to reach this point in its lifecycle, a number of governance
transitions must be performed in WSRR. Table 31 lists the transitions from a newly
created policy to a Monitor state according to the default WSRR governance
enablement profile:

Table 31. The transitions from a newly created policy to a monitored state.

WSRR Lifecycle Transition	Transition URI in WSRR event	Event handling in ITCAM for SOA
Authorize for Development	http://www.ibm.com/xmlns/prod/ serviceregistry/lifecycle/v6r3/ LifecycleDefinition#AuthorizeForDevelopment	Ignore
Approve for Deployment	http://www.ibm.com/xmlns/prod/ serviceregistry/lifecycle/v6r3/ LifecycleDefinition#ApproveForDeployment	Ignore
Approve for Production	http://www.ibm.com/xmlns/prod/ serviceregistry/lifecycle/v6r3/ LifecycleDefinition#ApproveForProduction	Process

WSRR Notification Event

When a policy transitions into the Monitor governance lifecycle state, WSRR sends
an XML notification to ITCAM for SOA, as shown in the following example:

```
<?xml version="1.0" encoding="utf-8"?>
<body:resources xmlns:body="http://www.ibm.com/xmlns/prod/serviceregistry/
HttpPostNotifierPluginMsgBody">
  <body:resource bsrURI="f1dbd3f1-94a4-44b2.bd6a.639695636a6c"
     correlationId="correlation-id1"
     securityToken="security-token1"
     type="Subscription">
    <body:notificationResource event="TRANSITION"
        resourceBsrURI=""
        resourceName=""
        resourceToSubscribedRelationship="attachedPolicy"
        resourceType="PolicyExpression"
        subscribedBsrUri="29243729-5334-44a7.9cf3.3e234b3ef38a"
        subscribedName="MySLD"
        subscribedPrimaryType=
           "http://www.ibm.com/xmlns/prod/serviceregistry/profile/v6r3/
GovernanceProfileExtensions#ServiceLevelDefinition"
        subscribedType="GenericObject"
        transition="http://www.ibm.com/xmlns/prod/serviceregistry/lifecycle/v6r3/
LifecycleDefinition#ApproveForProduction">
       <policyUri>urn:Fatal</policyUri>
    </body:notificationResource>
  </body:resource>
</body:resources>
```

Process Rule Definition

The default WSRR SDMS configuration file template includes the following process
rule definition:

```
<!-- ========================================================
Policy 'Approve for Production'
======================================================== -->
<process-rule event="TRANSITION"
   represents="SLD_Policy_Transition"
   startOn="create"
   operation="create"
   resourceToSubscribedRelationship="attachedPolicy"
   resourceType="PolicyExpression"
   transition="alias_v6r3.ld.approve.production">
   <rule-primary-types>
      <primary-types subscribedPrimaryType="alias_v6r3.gp.extensions.sld"/>
      <primary-types subscribedPrimaryType="alias_v6r3.ge.model.sld"/>
   </rule-primary-types>
   <classification-filters>
      <ref-classification-filter name="policy-expression-govn-cf"/>
      <ref-classification-filter name="sld-subscribable-govn-cf"/>
   </classification-filters>
   <relationship-filters>
      <relationship-filter appliesTo="ServiceLevelEntity"
         name="gep63_availableEndpoints" ordinality="1">
         <ref-classification-filter name="service-endpoint-envr-cf"/>
         <ref-classification-filter name="service-endpoint-online-cf"/>
      </relationship-filter>
      <relationship-filter appliesTo="ServiceLevelEntity"
         name="gep63_availableOperations" ordinality="0">
         <ref-classification-filter name="service-operation-envr-cf"/>
         <ref-classification-filter name="service-operation-govn-cf"/>
      </relationship-filter>
   </relationship-filters>
</process-rule>
```

This process rule defines the processing of events that represent the transition of an
SLM policy attached to a SLD to an approve for production lifecycle state. If the
event matches certain requirements, ITCAM for SOA creates a situation for the
policy.

In the example event, the SLD is identified by the following attribute:
`subscribedBsrUri="29243729-5334-44a7.9cf3.3e234b3ef38a".`

The SLM policy that is attached to the SLD is identified in the WSRR event by the `<policyUri>` element, for example:

`<policyUri>urn:Fatal</policyUri>`

The primary types determine that the process rules must be applied to SLDs:

```
<rule-primary-types>
    <primary-types subscribedPrimaryType="alias_v6r3.gp.extensions.sld"/>
    <primary-types subscribedPrimaryType="alias_v6r3.ge.model.sld"/>
</rule-primary-types>
```

The following attributes determine that the rule applies to a policy (`PolicyExpression`) that is attached to the SLD (`attachedPolicy`):

```
resourceToSubscribedRelationship="attachedPolicy"
resourceType="PolicyExpression">
```

The action to take (create and start situation) is determined by the combination of the following two attributes:

```
startOn="create"
operation="create"
```

The following requirements must be met:

- The SLD must be in a subscribable state. This requirement is enforced by the `sld-subscribable-govn-cf` classification filter reference:

  `<ref-classification-filter name="sld-subscribable-govn-cf"/>`

- The SLD must have a policy attachment with the policy classification URI. This requirement is enforced by the `policy-expression-govn-cf` classification filter:

  `<ref-classification-filter name="policy-expression-govn-cf"/>`

- The SLD must have at least one service endpoint associated with it. This requirement is defined by the relationship filter for the `gep63_availableEndpoints` entity of the SLD. This filter also references classification filters to ensure that the service endpoint is online and in one of the monitored environments:

  ```
  <relationship-filter appliesTo="ServiceLevelEntity"
      name="gep63_availableEndpoints" ordinality="1">
    <ref-classification-filter name="service-endpoint-envr-cf"/>
    <ref-classification-filter name="service-endpoint-online-cf"/>
  </relationship-filter>
  ```

- The SLD can have zero or more service operations associated with it. This requirement is defined by the relationship filter for the `gep63_availableOperations` entity of the SLD. This filter references classification filters to ensure that any service operation can be monitored according to its lifecycle stage and is in one of the monitored environments:

  ```
  <relationship-filter appliesTo="ServiceLevelEntity"
      name="gep63_availableOperations" ordinality="0">
    <ref-classification-filter name="service-operation-envr-cf"/>
    <ref-classification-filter name="service-operation-govn-cf"/>
  </relationship-filter>
  ```

Modifying the Process Rule

You might have to modify this process rule if WSRR has a custom governance enablement profile. In this case, ensure that all the URIs in the process rule (including the classification filters that it references) are valid in the custom profile.

Ensure that the URI of the WSRR lifecycle stage that triggers the process rule is correct in the following line:

```
transition="alias_v6r3.ld.approve.production"
```

If the existing value of the alias does not match the value in the governance enablement profile, change the alias to the new value. Alternatively, use the new value in the process rule instead of the alias.

Policy Approve Specification˝ Process Rule

The Policy Approve Specification˝ process rule determines the processing of the WSRR event that is generated when a Policy moves to an 'Approved' state as part of the policy governance lifecycle in WSRR. This process rule exists only for WSRR 8.0.

When ITCAM for SOA processes this event, it creates and starts situations for the SLM policy.

The WSRR event is identified as TRANSITION. The SLD is the subscribed primary type; the resource type is PolicyExpression.

WSRR Notification Event

When a policy transitions into the Approved governance lifecycle state, WSRR sends an XML notification to ITCAM for SOA, as shown in the following example:

```
<?xml version="1.0" encoding="utf-8"?>
<body:resources xmlns:body="http://www.ibm.com/xmlns/prod/serviceregistry/
HttpPostNotifierPluginMsgBody">
<body:resource bsrURI="f1dbd3f1-94a4-44b2.bd6a.639695636a6c"
    correlationId="correlation-id1"
    securityToken="security-token1"
    type="Subscription">
    <body:notificationResource event="TRANSITION"
      resourceBsrURI=""
      resourceName=""
      resourceToSubscribedRelationship="attachedPolicy"
      resourceType="PolicyExpression"
      subscribedBsrUri="29243729-5334-44a7.9cf3.3e234b3ef38a"
      subscribedName="MySLD"
      subscribedPrimaryType=
        "http://www.ibm.com/xmlns/prod/serviceregistry/profile/v6r3/
GovernanceProfileExtensions#ServiceLevelDefinition"
      subscribedType="GenericObject"
      transition="http://www.ibm.com/xmlns/prod/serviceregistry/lifecycle/v6r3/
LifecycleDefinition#ApproveSpecification">
      <policyUri>urn:Fatal</policyUri>
    </body:notificationResource>
</body:resource>
```

Process Rule Definition

The default WSRR SDMS configuration file template for WSRR 8.0 includes the following process rule definition:

```
<!-- =======================================================
   Policy ˙Approve Specification˙
   ======================================================= -->
<process-rule event="TRANSITION"
 represents="SLD_Policy_Transition"
 startOn="create"
 operation="create"
 resourceToSubscribedRelationship="attachedPolicy"
```

```
                 resourceType="PolicyExpression"
                 transition="alias_v6r3.ld.approve.specification">

                 <rule-primary-types>
                  <primary-types subscribedPrimaryType="alias_v6r3.gp.extensions.sld"/>
                  <primary-types subscribedPrimaryType="alias_v6r3.ge.model.sld"/>
                 </rule-primary-types>

                 <classification-filters>
                  <ref-classification-filter name="policy-expression-govn-cf"/>
                  <ref-classification-filter name="sld-subscribable-govn-cf"/>
                 </classification-filters>

                 <relationship-filters>

                  <relationship-filter appliesTo="ServiceLevelEntity"
                   name="gep63_availableEndpoints" ordinality="1">
                   <ref-classification-filter name="service-endpoint-envr-cf"/>
                   <ref-classification-filter name="service-endpoint-online-cf"/>
                  </relationship-filter>

                  <relationship-filter appliesTo="ServiceLevelEntity"
                    name="gep63_availableOperations" ordinality="0">
                   <ref-classification-filter name="service-operation-envr-cf"/>
                   <ref-classification-filter name="service-operation-govn-cf"/>
                  </relationship-filter>

                 </relationship-filters>
                </process-rule>
```

This process rule defines the processing of events that represent the transition of an SLM policy attached to a SLD to an approve specification lifecycle state. If the event matches certain requirements, ITCAM for SOA creates and starts a situation for the policy.

In the example event, the SLD is identified by the following attribute:

```
subscribedBsrUri="29243729-5334-44a7.9cf3.3e234b3ef38a".
```

The SLM policy that is attached to the SLD is identified in the WSRR event by the <policyUri> element, for example:

```
<policyUri>urn:Fatal</policyUri>
```

The primary types determine that the process rules must be applied to SLDs:

```
   <rule-primary-types>
      <primary-types subscribedPrimaryType="alias_v6r3.gp.extensions.sld"/>
      <primary-types subscribedPrimaryType="alias_v6r3.ge.model.sld"/>
   </rule-primary-types>
```

The following attributes determine that the rule applies to a policy (PolicyExpression) that is attached to the SLD (attachedPolicy):

```
resourceToSubscribedRelationship="attachedPolicy"
resourceType="PolicyExpression">
```

The action to take (create and start situation) is determined by the combination of the following two attributes:

```
startOn="create"
operation="create"
```

The following requirements must be met:

- The SLD must be in a subscribable state. This requirement is enforced by the `sld-subscribable-govn-cf` classification filter reference:

  ```
  <ref-classification-filter name="sld-subscribable-govn-cf"/>
  ```

- The SLD must have a policy attachment with the policy classification URI. This requirement is enforced by the `policy-expression-govn-cf` classification filter:

  ```
  <ref-classification-filter name="policy-expression-govn-cf"/>
  ```

- The SLD must have at least one service endpoint associated with it. This requirement is defined by the relationship filter for the `gep63_availableEndpoints` entity of the SLD. This filter also references classification filters to ensure that the service endpoint is online and in one of the monitored environments:

  ```
  <relationship-filter appliesTo="ServiceLevelEntity"
        name="gep63_availableEndpoints" ordinality="1">
     <ref-classification-filter name="service-endpoint-envr-cf"/>
     <ref-classification-filter name="service-endpoint-online-cf"/>
  </relationship-filter>
  ```

- The SLD can have zero or more service operations associated with it. This requirement is defined by the relationship filter for the `gep63_availableOperations` entity of the SLD. This filter references classification filters to ensure that any service operation can be monitored according to its lifecycle stage and is in one of the monitored environments:

  ```
  <relationship-filter appliesTo="ServiceLevelEntity"
        name="gep63_availableOperations" ordinality="0">
     <ref-classification-filter name="service-operation-envr-cf"/>
     <ref-classification-filter name="service-operation-govn-cf"/>
  </relationship-filter>
  ```

Modifying the Process Rule

You might have to modify this process rule if WSRR has a custom governance enablement profile. In this case, ensure that all the URIs in the process rule (including the classification filters that it references) are valid in the custom profile.

Ensure that the URI of the WSRR lifecycle stage that triggers the process rule is correct in the following line:

```
transition="alias_v6r3.ld.approve.specification"
```

If the existing value of the alias does not match the value in the governance enablement profile, change the alias to the new value. Alternatively, use the new value in the process rule instead of the alias.

Policy 'Retire from Use' Process Rule

The Policy 'Retire from Use' process rule determines the processing of the WSRR event that is generated when a Service Level Monitoring policy lifecycle transitions to a Policy Retired governance state.

When ITCAM for SOA processes this event, it deletes situations for the SLM policy and SLD.

The WSRR event is identified as TRANSITION. The SLD is the subscribed primary type; the resource type is PolicyExpression.

Table 32 on page 82 lists the processing of the WSRR event notification:

Table 32. ITCAM for SOA processing of retiring a policy from use.

WSRR action	WSRR event	Event handling in ITCAM for SOA
Retire from Use	http://www.ibm.com/xmlns/prod/ serviceregistry/lifecycle/v6r3/ LifecycleDefinition#RetireFromUse	Process

WSRR Notification Event

When an SLM policy transitions to a 'Policy Retired' governance state, WSRR sends an XML notification to ITCAM for SOA, as shown in the following example:

```
<?xml version="1.0" encoding="utf-8"?>
<body:resources xmlns:body="http://www.ibm.com/xmlns/prod/serviceregistry/
HttpPostNotifierPluginMsgBody">
  <body:resource bsrURI="f1dbd3f1-94a4-44b2.bd6a.639695636a6c"
    correlationId="correlation-id1"
    securityToken="security-token1"
    type="Subscription">
    <body:notificationResource event="TRANSITION"
      resourceBsrURI=""
      resourceName=""
      resourceToSubscribedRelationship="attachedPolicy"
      resourceType="PolicyExpression"
      subscribedBsrUri="29243729-5334-44a7.9cf3.3e234b3ef38a"
      subscribedName="MySLD"
      subscribedPrimaryType=
          "http://www.ibm.com/xmlns/prod/serviceregistry/profile/v6r3/
GovernanceProfileExtensions#ServiceLevelDefinition"
      subscribedType="GenericObject"
      transition="http://www.ibm.com/xmlns/prod/serviceregistry/lifecycle/v6r3/
LifecycleDefinition#RetireFromUse">
      <policyUri>urn:Fatal</policyUri>
    </body:notificationResource>
  </body:resource>
</body:resources>
```

Process Rule Definition

The default WSRR SDMS configuration file template includes the following process rule definition:

```
<!-- =========================================================
Policy 'Retire from Use'
========================================================= -->
<process-rule event="TRANSITION"
   represents="SLD_Policy_Transition"
   operation="delete"
   resourceToSubscribedRelationship="attachedPolicy"
   resourceType="PolicyExpression"
   transition="alias_v6r3.ld.retire.from.use">
   <rule-primary-types>
      <primary-types subscribedPrimaryType="alias_v6r3.gp.extensions.sld"/>
      <primary-types subscribedPrimaryType="alias_v6r3.ge.model.sld"/>
   </rule-primary-types>
</process-rule>
```

This process rule defines the processing of events that represent the transition of an SLM policy to a policy retired state. ITCAM for SOA deletes any situations that were created for the policy and the SLD.

In the example event, the SLD is identified by the following attribute:

```
subscribedBsrUri="29243729-5334-44a7.9cf3.3e234b3ef38a".
```

The SLM policy that is attached to the SLD is identified in the WSRR event by the <policyUri> element, for example:

```
<policyUri>urn:Fatal</policyUri>
```

The primary types determine that the process rules must be applied to SLDs:

```
<rule-primary-types>
    <primary-types subscribedPrimaryType="alias_v6r3.gp.extensions.sld"/>
    <primary-types subscribedPrimaryType="alias_v6r3.ge.model.sld"/>
</rule-primary-types>
```

The following attributes determine that the rule applies to a policy (`PolicyExpression`) that is attached to the SLD (`attachedPolicy`):

```
resourceToSubscribedRelationship="attachedPolicy"
resourceType="PolicyExpression">
```

The action to take (delete situations) is determined by the following attribute:

```
operation="delete"
```

Policy 'Revoke' Process Rule

The Policy 'Revoke' process rule determines the processing of the WSRR event that is generated when a Service Level Monitoring policy is revoked with the 'Revoke' lifecycle transition.

When ITCAM for SOA processes this event, it deletes situations for the SLM policy and SLD.

The WSRR event is identified as TRANSITION. The SLD is the subscribed primary type; the resource type is PolicyExpression.

Table 33 lists the processing of the WSRR event notification:

Table 33. ITCAM for SOA handling of revoking a policy.

WSRR action	WSRR event	Event processing in ITCAM for SOA
Revoke	`transition = http://www.ibm.com/xmlns` `/prod/serviceregistry/lifecycle/v6r3/` `  LifecycleDefinition#Revoke` `resourceToSubscribedRelationship=` `  "attachedPolicy"` `resourceType="PolicyExpression"` `subscribedPrimaryType=<SLD URI>`	Process

WSRR Notification Event

When an SLM policy is revoked, WSRR sends an XML notification to ITCAM for SOA, as shown in the following example:

```
<?xml version="1.0" encoding="utf-8"?>
<body:resources xmlns:body="http://www.ibm.com/xmlns/prod/serviceregistry/
HttpPostNotifierPluginMsgBody">
  <body:resource bsrURI="f1dbd3f1-94a4-44b2.bd6a.639695636a6c"
    correlationId="correlation-id1"
    securityToken="security-token1"
    type="Subscription">
    <body:notificationResource event="TRANSITION"
        resourceBsrURI=""
```

```
            resourceName=""
            resourceToSubscribedRelationship="attachedPolicy"
            resourceType="PolicyExpression"
            subscribedBsrUri="29243729-5334-44a7.9cf3.3e234b3ef38a"
            subscribedName="MySLD"
            subscribedPrimaryType=
                "http://www.ibm.com/xmlns/prod/serviceregistry/profile/v6r3/
GovernanceProfileExtensions#ServiceLevelDefinition"
            subscribedType="GenericObject"
            transition="http://www.ibm.com/xmlns/prod/serviceregistry/lifecycle/
v6r3/LifecycleDefinition#Revoke">
          <policyUri>urn:Fatal</policyUri>
        </body:notificationResource>
      </body:resource>
</body:resources>
```

Process Rule Definition

The default WSRR SDMS configuration file template includes the following process rule definition:

```
<!-- =======================================================
Policy 'Revoke'
======================================================= -->
<process-rule event="TRANSITION"
    represents="SLD_Policy_Transition"
    operation="delete"
    resourceToSubscribedRelationship="attachedPolicy"
    resourceType="PolicyExpression"
    transition="alias_v6r3.ld.revoke">
    <rule-primary-types>
        <primary-types subscribedPrimaryType="alias_v6r3.gp.extensions.sld"/>
        <primary-types subscribedPrimaryType="alias_v6r3.ge.model.sld"/>
    </rule-primary-types>
</process-rule>
```

This process rule defines the processing of events that represent the transition of an SLM policy to a revoked state. ITCAM for SOA deletes any situations that were created for the policy.

In the example event, the SLD is identified by the following attribute:

`subscribedBsrUri="29243729-5334-44a7.9cf3.3e234b3ef38a".`

The SLM policy that is attached to the SLD is identified in the WSRR event by the <policyUri> element, for example:

`<policyUri>urn:Fatal</policyUri>`

The primary types determine that the process rules must be applied to SLDs:

```
    <rule-primary-types>
        <primary-types subscribedPrimaryType="alias_v6r3.gp.extensions.sld"/>
        <primary-types subscribedPrimaryType="alias_v6r3.ge.model.sld"/>
    </rule-primary-types>
```

The following attributes determine that the rule applies to a policy (PolicyExpression) that is attached to the SLD (attachedPolicy):

```
resourceToSubscribedRelationship="attachedPolicy"
resourceType="PolicyExpression">
```

The action to take (delete situations) is determined by the following attribute:

`operation="delete"`

Policy 'Deprecate' Process Rule

The Policy 'Deprecate' process rule determines the processing of the WSRR event that is generated when a Service Level Monitoring policy lifecycle transitions to a Deprecated governance state. This process rule exists only for WSRR 8.0.

When ITCAM for SOA processes this event, it deletes situations for the SLM policy and SLD.

The WSRR event is identified as TRANSITION. The SLD is the subscribed primary type; the resource type is PolicyExpression.

WSRR Notification Event

When an SLM policy transitions to a 'Deprecated' governance state, WSRR sends an XML notification to ITCAM for SOA, as shown in the following example:

```
<?xml version="1.0" encoding="utf-8"?>
<body:resources xmlns:body="http://www.ibm.com/xmlns/prod/serviceregistry/
HttpPostNotifierPluginMsgBody">
   <body:resource bsrURI="f1dbd3f1-94a4-44b2.bd6a.639695636a6c"
      correlationId="correlation-id1"
      securityToken="security-token1"
      type="Subscription">
      <body:notificationResource event="TRANSITION"
         resourceBsrURI=""
   resourceName=""
   resourceToSubscribedRelationship="attachedPolicy"
   resourceType="PolicyExpression"
   subscribedBsrUri="29243729-5334-44a7.9cf3.3e234b3ef38a"
   subscribedName="MySLD"
   subscribedPrimaryType=
  "http://www.ibm.com/xmlns/prod/serviceregistry/profile/v6r3/
GovernanceProfileExtensions#ServiceLevelDefinition"
   subscribedType="GenericObject"
   transition="http://www.ibm.com/xmlns/prod/serviceregistry/lifecycle/v6r3/
LifecycleDefinition#Deprecated">
   <policyUri>urn:Fatal</policyUri>
      </body:notificationResource>
   </body:resource>
</body:resources>
```

Process Rule Definition

The default WSRR SDMS configuration file template for WSRR 8.0 includes the following process rule definition:

```
<!-- =======================================================
 Policy 'Deprecate'
 ======================================================= -->
<process-rule event="TRANSITION"
 represents="SLD_Policy_Transition"
      operation="delete"
      resourceToSubscribedRelationship="attachedPolicy"
      resourceType="PolicyExpression"
      transition="alias_v6r3.ld.deprecate">
      <rule-primary-types>
         <primary-types subscribedPrimaryType="alias_v6r3.gp.extensions.sld"/>
         <primary-types subscribedPrimaryType="alias_v6r3.ge.model.sld"/>
      </rule-primary-types>
</process-rule>
```

This process rule defines the processing of events that represent the transition of an SLM policy to a deprecated state. ITCAM for SOA deletes any situations that were created for the policy and the SLD.

In the example event, the SLD is identified by the following attribute:

`subscribedBsrUri="29243729-5334-44a7.9cf3.3e234b3ef38a".`

The SLM policy that is attached to the SLD is identified in the WSRR event by the <policyUri> element, for example:

`<policyUri>urn:Fatal</policyUri>`

The primary types determine that the process rules must be applied to SLDs:

```
<rule-primary-types>
    <primary-types subscribedPrimaryType="alias_v6r3.gp.extensions.sld"/>
    <primary-types subscribedPrimaryType="alias_v6r3.ge.model.sld"/>
</rule-primary-types>
```

The following attributes determine that the rule applies to a policy (PolicyExpression) that is attached to the SLD (attachedPolicy):

```
resourceToSubscribedRelationship="attachedPolicy"
resourceType="PolicyExpression">
```

The action to take (delete situations) is determined by the following attribute:

`operation="delete"`

Policy 'Redefine' Process Rule

The Policy 'Redefine' process rule determines the processing of the WSRR event that is generated when a Service Level Monitoring policy is redefined. This process rule exists only for WSRR 8.0.

When ITCAM for SOA processes this event, it deletes situations for the SLM policy and SLD.

The WSRR event is identified as TRANSITION. The SLD is the subscribed primary type; the resource type is PolicyExpression.

WSRR Notification Event

When an SLM policy is redefined, WSRR sends an XML notification to ITCAM for SOA, as shown in the following example:

```
<?xml version="1.0" encoding="utf-8"?>
<body:resources xmlns:body="http://www.ibm.com/xmlns/prod/serviceregistry/
HttpPostNotifierPluginMsgBody">
   <body:resource bsrURI="f1dbd3f1-94a4-44b2.bd6a.639695636a6c"
      correlationId="correlation-id1"
      securityToken="security-token1"
      type="Subscription">
      <body:notificationResource event="TRANSITION"
          resourceBsrURI=""
   resourceName=""
   resourceToSubscribedRelationship="attachedPolicy"
   resourceType="PolicyExpression"
   subscribedBsrUri="29243729-5334-44a7.9cf3.3e234b3ef38a"
   subscribedName="MySLD"
   subscribedPrimaryType=
  "http://www.ibm.com/xmlns/prod/serviceregistry/profile/v6r3/
GovernanceProfileExtensions#ServiceLevelDefinition"
   subscribedType="GenericObject"
```

```
    transition="http://www.ibm.com/xmlns/prod/serviceregistry/lifecycle/v6r3/
LifecycleDefinition#Redefine">
    <policyUri>urn:Fatal</policyUri>
        </body:notificationResource>
    </body:resource>
</body:resources>
```

Process Rule Definition

The default WSRR SDMS configuration file template for WSRR 8.0 includes the
following process rule definition:

```
<!-- ========================================================
 Policy 'Redefine'
======================================================== -->
<process-rule event="TRANSITION"
 represents="SLD_Policy_Transition"
 operation="delete"
 resourceToSubscribedRelationship="attachedPolicy"
 resourceType="PolicyExpression"
 transition="alias_v6r3.ld.redefine">
 <rule-primary-types>
  <primary-types subscribedPrimaryType="alias_v6r3.gp.extensions.sld"/>
  <primary-types subscribedPrimaryType="alias_v6r3.ge.model.sld"/>
 </rule-primary-types>
</process-rule>|
```

This process rule defines the processing of events that represent the redefine
transition of an SLM policy. ITCAM for SOA deletes any situations that were
created for the policy and the SLD.

In the example event, the SLD is identified by the following attribute:

```
subscribedBsrUri="29243729-5334-44a7.9cf3.3e234b3ef38a".
```

The SLM policy that is attached to the SLD is identified in the WSRR event by the
<policyUri> element, for example:

```
<policyUri>urn:Fatal</policyUri>
```

The primary types determine that the process rules must be applied to SLDs:

```
    <rule-primary-types>
        <primary-types subscribedPrimaryType="alias_v6r3.gp.extensions.sld"/>
        <primary-types subscribedPrimaryType="alias_v6r3.ge.model.sld"/>
    </rule-primary-types>
```

The following attributes determine that the rule applies to a policy
(PolicyExpression) that is attached to the SLD (attachedPolicy):

```
resourceToSubscribedRelationship="attachedPolicy"
resourceType="PolicyExpression">
```

The action to take (delete situations) is determined by the following attribute:

```
operation="delete"
```

Policy 'Supercede' Process Rule

The Policy 'Supercede' process rule determines the processing of the WSRR event
that is generated when a Service Level Monitoring policy is superceded. This
process rule exists only for WSRR 8.0.

When ITCAM for SOA processes this event, it stops situations for the SLM policy
and SLD.

The WSRR event is identified as TRANSITION. The SLD is the subscribed primary type; the resource type is PolicyExpression.

WSRR Notification Event

When an SLM policy is superceded, WSRR sends an XML notification to ITCAM for SOA, as shown in the following example:

```
<?xml version="1.0" encoding="utf-8"?>
<body:resources xmlns:body="http://www.ibm.com/xmlns/prod/serviceregistry/
HttpPostNotifierPluginMsgBody">
   <body:resource bsrURI="f1dbd3f1-94a4-44b2.bd6a.639695636a6c"
      correlationId="correlation-id1"
      securityToken="security-token1"
      type="Subscription">
      <body:notificationResource event="TRANSITION"
         resourceBsrURI=""
   resourceName=""
   resourceToSubscribedRelationship="attachedPolicy"
   resourceType="PolicyExpression"
   subscribedBsrUri="29243729-5334-44a7.9cf3.3e234b3ef38a"
   subscribedName="MySLD"
   subscribedPrimaryType=
  "http://www.ibm.com/xmlns/prod/serviceregistry/profile/v6r3/
GovernanceProfileExtensions#ServiceLevelDefinition"
   subscribedType="GenericObject"
   transition="http://www.ibm.com/xmlns/prod/serviceregistry/lifecycle/v6r3/
LifecycleDefinition#Supercede">
   <policyUri>urn:Fatal</policyUri>
      </body:notificationResource>
   </body:resource>
</body:resources>
```

Process Rule Definition

The default WSRR SDMS configuration file template for WSRR 8.0 includes the following process rule definition:

```
<!-- =========================================================
   Policy `Supercede`
   ========================================================= -->
<process-rule event="TRANSITION"
   represents="SLD_Policy_Transition"
   operation="stop"
   resourceToSubscribedRelationship="attachedPolicy"
   resourceType="PolicyExpression"
   transition="alias_v6r3.ld.supersede">
   <situation-configuration>
      <property name="situation.run.at.startup" value="false"/>
   </situation-configuration>
   <rule-primary-types>
      <primary-types subscribedPrimaryType="alias_v6r3.gp.extensions.sld"/>
      <primary-types subscribedPrimaryType="alias_v6r3.ge.model.sld"/>
   </rule-primary-types>
</process-rule>
```

This process rule defines the processing of events that represent the supercede transition of an SLM policy. ITCAM for SOA stops any situations that were created for the policy and the SLD.

In the example event, the SLD is identified by the following attribute:

```
subscribedBsrUri="29243729-5334-44a7.9cf3.3e234b3ef38a".
```

The SLM policy that is attached to the SLD is identified in the WSRR event by the <policyUri> element, for example:

```
<policyUri>urn:Fatal</policyUri>
```

The primary types determine that the process rules must be applied to SLDs:

```
<rule-primary-types>
    <primary-types subscribedPrimaryType="alias_v6r3.gp.extensions.sld"/>
    <primary-types subscribedPrimaryType="alias_v6r3.ge.model.sld"/>
</rule-primary-types>
```

The following attributes determine that the rule applies to a policy (PolicyExpression) that is attached to the SLD (attachedPolicy):

```
resourceToSubscribedRelationship="attachedPolicy"
resourceType="PolicyExpression">
```

The action to take (delete situations) is determined by the following attribute:

```
operation="stop"
```

Policy 'Update' Process Rule

The Policy 'Update' process rule determines the processing of the WSRR event that is generated when a policy is edited in WSRR. This includes the editing of policy properties, relationships, classifications, or content.

When a policy is updated, a separate WSRR event is generated for each of the SLDs to which the policy is attached.

When ITCAM for SOA processes this event, it creates the situations for this SLD if they do not exist, or updates them if they exist.

The WSRR event is identified as UPDATE. The SLD is the subscribed primary type in the event. The resource type is PolicyExpression, and the relationship between the resource and the subscribed entity is attachedPolicy.

Table 34 lists the handling of the WSRR event notification:

Table 34. ITCAM for SOA handling of updating a policy.

WSRR action	WSRR event	Event handling in ITCAM for SOA
Edit Policy	event='UPDATE' resourceType='PolicyExpression' resourceToSubscribedRelationship= "attachedPolicy" subscribedPrimaryType= <SLD classification URI>	Process

WSRR Notification Event

When an SLM policy attached to an SLD is updated, WSRR sends an XML notification to ITCAM for SOA, as shown in the following example:

```
<?xml version="1.0" encoding="utf-8"?>
<body:resources xmlns:body="http://www.ibm.com/xmlns/prod/serviceregistry/
HttpPostNotifierPluginMsgBody">
  <body:resource bsrURI="f1dbd3f1-94a4-44b2.bd6a.639695636a6c"
    correlationId="correlation-id1"
    securityToken="security-token1"
    type="Subscription">
```

```
      <body:notificationResource event="UPDATE"
          resourceBsrURI=""
          resourceName=""
          resourceToSubscribedRelationship="attachedPolicy"
          resourceType="PolicyExpression"
          subscribedBsrUri="4e4f314e-f180-40ef.9c78.eb59a9eb7842"
          subscribedName="MySLD"
          subscribedPrimaryType=
              "http://www.ibm.com/xmlns/prod/serviceregistry/profile/v6r3/
GovernanceProfileExtensions#ServiceLevelDefinition"
          subscribedType="GenericObject">
        <policyUri>urn:Fatal</policyUri>
      </body:notificationResource>
    </body:resource>
</body:resources>
```

Process Rule Definition

The default WSRR SDMS configuration file template includes the following process
rule definition:

```
<!-- ========================================================
Policy `Update`
======================================================= -->
<process-rule event="UPDATE"
   represents="SLD_Policy_Update"
   startOn="createOrUpdate"
   operation="createOrUpdate"
   resourceToSubscribedRelationship="attachedPolicy"
   resourceType="PolicyExpression">
   <rule-primary-types>
      <primary-types subscribedPrimaryType="alias_v6r3.gp.extensions.sld"/>
      <primary-types subscribedPrimaryType="alias_v6r3.ge.model.sld"/>
   </rule-primary-types>
   <classification-filters>
       <ref-classification-filter name="sld-subscribable-govn-cf"/>
      <ref-classification-filter name="policy-expression-govn-cf"/>
    </classification-filters>
   <relationship-filters>
      <relationship-filter appliesTo="ServiceLevelEntity"
         name="gep63_availableEndpoints" ordinality="1">
         <ref-classification-filter name="service-endpoint-envr-cf"/>
         <ref-classification-filter name="service-endpoint-online-cf"/>
      </relationship-filter>
      <relationship-filter appliesTo="ServiceLevelEntity"
         name="gep63_availableOperations" ordinality="0">
         <ref-classification-filter name="service-operation-envr-cf"/>
         <ref-classification-filter name="service-operation-govn-cf"/>
      </relationship-filter>
   </relationship-filters>
</process-rule>
```

This process rule defines the processing of events that represent the updating of an
SLM policy attached to an SLD. If the event matches certain requirements, ITCAM
for SOA creates or updates situations for the policy and SLD.

In the example event, the SLD is identified by the following attribute:

`subscribedBsrUri="29243729-5334-44a7.9cf3.3e234b3ef38a".`

The SLM policy that is attached to the SLD is identified in the WSRR event by the
<policyUri> element, for example:

`<policyUri>urn:Fatal</policyUri>`

The primary types determine that the process rules must be applied to SLDs:

```
<rule-primary-types>
    <primary-types subscribedPrimaryType="alias_v6r3.gp.extensions.sld"/>
    <primary-types subscribedPrimaryType="alias_v6r3.ge.model.sld"/>
</rule-primary-types>
```

The following attributes determine that the rule applies to a policy (PolicyExpression) that is attached to the SLD (attachedPolicy):

```
resourceToSubscribedRelationship="attachedPolicy"
resourceType="PolicyExpression">
```

The action to take (create and start or update situations) is determined by the combination of the following two attributes:

```
startOn="createOrUpdate"
operation="createOrUpdate"
```

The following requirements must be met:

- The SLD must be in a subscribable state. This requirement is enforced by the `sld-subscribable-govn-cf` classification filter reference:

  ```
  <ref-classification-filter name="sld-subscribable-govn-cf"/>
  ```

- The SLD must have a policy attachment with the policy classification URI. This requirement is enforced by the `policy-expression-govn-cf` classification filter:

  ```
  <ref-classification-filter name="policy-expression-govn-cf"/>
  ```

- The SLD must have at least one service endpoint associated with it. This requirement is defined by the relationship filter for the `gep63_availableEndpoints` entity of the SLD. This filter also references classification filters to ensure that the service endpoint is online and in one of the monitored environments:

  ```
  <relationship-filter appliesTo="ServiceLevelEntity"
      name="gep63_availableEndpoints" ordinality="1">
    <ref-classification-filter name="service-endpoint-envr-cf"/>
    <ref-classification-filter name="service-endpoint-online-cf"/>
  </relationship-filter>
  ```

- The SLD can have zero or more service operations associated with it. This requirement is defined by the relationship filter for the `gep63_availableOperations` entity of the SLD. This filter references classification filters to ensure that any service operation can be monitored according to its lifecycle stage and is in one of the monitored environments:

  ```
  <relationship-filter appliesTo="ServiceLevelEntity"
      name="gep63_availableOperations" ordinality="0">
    <ref-classification-filter name="service-operation-envr-cf"/>
    <ref-classification-filter name="service-operation-govn-cf"/>
  </relationship-filter>
  ```

Service Endpoint 'Approve for use' Process Rule

The Service Endpoint 'Approve for Use' process rule determines the processing of the WSRR event that is generated when a Service Endpoint moves to an 'Online' state as part of its governance lifecycle in WSRR.

When a Service Endpoint becomes Online, it means that mediations can consider this endpoint as a possible routing target.

When ITCAM for SOA processes this event, it creates situations for any policy attachments on any SLD with which the Service Endpoint is associated.

Table 35 on page 92 lists the processing of the WSRR event notification:

Table 35. ITCAM for SOA processing of approving a service endpoint for use.

WSRR action	WSRR event	Event processing in ITCAM for SOA
Service Endpoint Approve for Use	transition=http://www.ibm.com/xmlns/ prod/serviceregistry/lifecycle/v6r3/ LifecycleDefinition#ApproveForUse	Process

WSRR Notification Event

When a Service Endpoint is approved for use, WSRR sends an XML notification to ITCAM for SOA, as shown in the following example:

```
<?xml version="1.0" encoding="utf-8"?>
<body:resources xmlns:body="http://www.ibm.com/xmlns/prod/serviceregistry/
HttpPostNotifierPluginMsgBody">
  <body:resource bsrURI="f1dbd3f1-94a4-44b2.bd6a.639695636a6c"
    correlationId="correlation-id1"
    securityToken="security-token1"
    type="Subscription">
    <body:notificationResource event="TRANSITION"
      resourceBsrURI="6dff3b6d-c31f-4f22.8c44.bfdeccbf4432"
      resourceName="se_mq2"
      resourcePrimaryType=
        "http://www.ibm.com/xmlns/prod/serviceregistry/v6r3/ServiceModel#
MQServiceEndpoint"
      resourceToSubscribedRelationship="sameObject"
      resourceType="GenericObject"
      subscribedBsrUri="6dff3b6d-c31f-4f22.8c44.bfdeccbf4432"
      subscribedName="se_mq2"
      subscribedPrimaryType="http://www.ibm.com/xmlns/prod/serviceregistry/
v6r3/ServiceModel#MQServiceEndpoint"
      subscribedType="GenericObject"
      transition="http://www.ibm.com/xmlns/prod/serviceregistry/lifecycle/
v6r3/LifecycleDefinition#ApproveForUse"/>
  </body:resource>
</body:resources>
```

Process Rule Definition

The default WSRR SDMS configuration file template includes the following process rule definition:

```
<!-- ==========================================================
Service Endpoint 'Approve for Use'
========================================================== -->
<process-rule event="TRANSITION"
  represents="SLD_Relation_Transition"
  startOn="create"
  operation="create"
  resourceToSubscribedRelationship="sameObject"
  transition="alias_v6r3.ld.approve.for.use">
  <rule-primary-types>
    <primary-types resourcePrimaryType="alias_v6r3.sm.soap.service.endpoint"
                   subscribedPrimaryType="alias_v6r3.sm.soap.service.endpoint"/>
    <primary-types resourcePrimaryType="alias_v6r3.sm.mq.service.endpoint"
                   subscribedPrimaryType="alias_v6r3.sm.mq.service.endpoint"/>
    <primary-types resourcePrimaryType="alias_v6r3.sm.extension.service.endpoint"
                   subscribedPrimaryType="alias_v6r3.sm.extension.service.endpoint"/>
  </rule-primary-types>
  <classification-filters>
    <ref-classification-filter name="sld-subscribable-govn-cf"/>
    <ref-classification-filter name="policy-expression-govn-cf"/>
  </classification-filters>
  <relationship-filters>
```

```
        <relationship-filter appliesTo="ServiceLevelEntity"
            name="gep63_availableEndpoints" ordinality="1">
          <ref-classification-filter name="service-endpoint-envr-cf"/>
          <ref-classification-filter name="service-endpoint-online-cf"/>
        </relationship-filter>
        <relationship-filter appliesTo="ServiceLevelEntity"
            name="gep63_availableOperations" ordinality="0">
          <ref-classification-filter name="service-operation-envr-cf"/>
          <ref-classification-filter name="service-operation-govn-cf"/>
        </relationship-filter>
    </relationship-filters>
</process-rule>
```

This process rule defines the processing of events that represent the transition of a Service Endpoint to an approve for use lifecycle state. If the event matches certain requirements, ITCAM for SOA creates situations for any policy attachments on any SLD with which the Service Endpoint is associated.

In the example event, the Service Endpoint is identified by the following attribute:

```
subscribedBsrUri="6dff3b6d-c31f-4f22.8c44.bfdeccbf4432"
```

The primary types determine that the process rule must be applied to SOAP, MQ, or Extension service endpoints:

```
<rule-primary-types>
    <primary-types resourcePrimaryType="alias_v6r3.sm.soap.service.endpoint"
                   subscribedPrimaryType="alias_v6r3.sm.soap.service.endpoint"/>
    <primary-types resourcePrimaryType="alias_v6r3.sm.mq.service.endpoint"
                   subscribedPrimaryType="alias_v6r3.sm.mq.service.endpoint"/>
    <primary-types resourcePrimaryType="alias_v6r3.sm.extension.service.endpoint"
                   subscribedPrimaryType="alias_v6r3.sm.extension.service.endpoint"/>
</rule-primary-types>
```

The action to take (create and start situations) is determined by the combination of the following two attributes:

```
startOn="create"
operation="create"
```

The following requirements must be satisfied:
- The SLD must be in a subscribable state. This requirement is enforced by the `sld-subscribable-govn-cf` classification filter reference:

  ```
  <ref-classification-filter name="sld-subscribable-govn-cf"/>
  ```
- The SLD must have a policy attachment with the policy classification URI. This requirement is enforced by the `policy-expression-govn-cf` classification filter:

  ```
  <ref-classification-filter name="policy-expression-govn-cf"/>
  ```
- The SLD must have at least one service endpoint associated with it. This requirement is defined by the relationship filter for the `gep63_availableEndpoints` entity of the SLD. This filter also references classification filters to ensure that the service endpoint is online and in one of the monitored environments:

  ```
  <relationship-filter appliesTo="ServiceLevelEntity"
        name="gep63_availableEndpoints" ordinality="1">
    <ref-classification-filter name="service-endpoint-envr-cf"/>
    <ref-classification-filter name="service-endpoint-online-cf"/>
  </relationship-filter>
  ```
- The SLD can have zero or more service operations associated with it. This requirement is defined by the relationship filter for the `gep63_availableOperations` entity of the SLD. This filter references classification

filters to ensure that any service operation can be monitored according to its lifecycle stage and is in one of the monitored environments:

```
<relationship-filter appliesTo="ServiceLevelEntity"
     name="gep63_availableOperations" ordinality="0">
  <ref-classification-filter name="service-operation-envr-cf"/>
  <ref-classification-filter name="service-operation-govn-cf"/>
</relationship-filter>
```

Modifying the Process Rule

You might have to modify this process rule if WSRR has a custom governance enablement profile.

In this case, you must ensure the following conditions are met:
- All the URIs in the process rule (including the classification filters that it references) are valid in the custom profile.
- The primary types section of the process rule lists all the valid service endpoint types.

Ensure that the URI of the WSRR lifecycle stage that triggers the process rule is correct in the following line:

```
transition="alias_v6r3.ld.approve.for.use"
```

If the existing value of the alias does not match the value in the governance enablement profile, change the alias to the new value. Alternatively, use the new value in the process rule instead of the alias.

If new Service Endpoint types were added to the custom governance enablement profile, add them under the <rule-primary-types> tag, so that the process rule can include the new type when its checks the event.

To add a Service Endpoint type, you must know its classification URI. You can obtain the URI from the governance enablement profile. Then, add it to the primary types:

```
<rule-primary-types
  <primary-types resourcePrimaryType="alias_v6r3.sm.soap.service.endpoint"
    subscribedPrimaryType="alias_v6r3.sm.soap.service.endpoint"/>
  <primary-types resourcePrimaryType="alias_v6r3.sm.mq.service.endpoint"
    subscribedPrimaryType="alias_v6r3.sm.mq.service.endpoint"/>
  <primary-types resourcePrimaryType="alias_v6r3.sm.extension.service.endpoint"
    subscribedPrimaryType="alias_v6r3.sm.extension.service.endpoint"/>
  <primary-types resourcePrimaryType="<Service Endpoint classification URI>"
    subscribedPrimaryType="<Service Endpoint classification URI>"/>
</rule-primary-types>
```

You can also create an alias for the new Service Endpoint type, under the <aliases> tag:

```
alias name="new_se_type" value=<Service Endpoint classification URI>
```

Then, you can reference the alias in the new <primary-types> tag:

```
  <primary-types resourcePrimaryType="alias_new_se_type"
    subscribedPrimaryType="alias_new_se_type"/>
```

If any Service Endpoint types are restricted in the custom governance profile, you can remove them from the rule primary types. For example, the following primary types definition means that only SOAP service endpoints trigger the process rule:

```
<rule-primary-types
  <primary-types resourcePrimaryType="alias_v6r3.sm.soap.service.endpoint
    subscribedPrimaryType="alias_v6r3.sm.soap.service.endpoint
</rule-primary-types>
```

Service Endpoint 'Revoke from Use' Process Rule

The Service Endpoint 'Revoke from Use' process rule determines the processing of
the WSRR event that is generated when a Service Endpoint moves to an Offline
state as part of its governance lifecycle in WSRR.

An offline endpoint might be deployed and thus reachable by potential consumers,
but if protected by mediations that can access the endpoint state, access to this
particular endpoint is denied.

When ITCAM for SOA processes this event, it deletes situations that were created
for any policy attachments on any SLD with which the Service Endpoint is
associated.

Table 36 lists the processing of the WSRR event notification:

Table 36. ITCAM for SOA processing of revoking a service endpoint from use.

WSRR action	WSRR event	Event processing in ITCAM for SOA
Service Endpoint Revoke from Use	transition=http://www.ibm.com/xmlns/ prod/serviceregistry/lifecycle/v6r3/ LifecycleDefinition#RevokeFromUse	Process

WSRR Notification Event

When a Service Endpoint is revoked from use, WSRR sends an XML notification to
ITCAM for SOA, as shown in the following example:

```
<?xml version="1.0" encoding="utf-8"?>
<body:resources xmlns:body="http://www.ibm.com/xmlns/prod/serviceregistry/
HttpPostNotifierPluginMsgBody">
  <body:resource bsrURI="f1dbd3f1-94a4-44b2.bd6a.639695636a6c"
    correlationId="correlation-id1"
    securityToken="security-token1"
    type="Subscription">
    <body:notificationResource event="TRANSITION"
      resourceBsrURI="6dff3b6d-c31f-4f22.8c44.bfdeccbf4432"
      resourceName="se_mq2"
      resourcePrimaryType="http://www.ibm.com/xmlns/prod/serviceregistry/
v6r3/ServiceModel#MQServiceEndpoint"
      resourceToSubscribedRelationship="sameObject"
      resourceType="GenericObject"
      subscribedBsrUri="6dff3b6d-c31f-4f22.8c44.bfdeccbf4432"
      subscribedName="se_mq2"
      subscribedPrimaryType="http://www.ibm.com/xmlns/prod/serviceregistry/
v6r3/ServiceModel#MQServiceEndpoint"
      subscribedType="GenericObject"
      transition="http://www.ibm.com/xmlns/prod/serviceregistry/lifecycle/
v6r3/LifecycleDefinition#RevokeFromUse"/>
  </body:resource>
</body:resources>
```

Process Rule Definition

The default WSRR SDMS configuration file template includes the following process
rule definition:

```
<!-- =======================================================
Service Endpoint 'Revoke from Use'
======================================================= -->
<process-rule event="TRANSITION"
   represents="SLD_Relation_Transition"
   operation="delete"
   resourceToSubscribedRelationship="sameObject"
   transition="alias_v6r3.ld.revoke.from.use">
   <rule-primary-types>
      <primary-types resourcePrimaryType="alias_v6r3.sm.soap.service.endpoint"
                     subscribedPrimaryType="alias_v6r3.sm.soap.service.endpoint"/>
      <primary-types resourcePrimaryType="alias_v6r3.sm.mq.service.endpoint"
                     subscribedPrimaryType="alias_v6r3.sm.mq.service.endpoint"/>
      <primary-types resourcePrimaryType="alias_v6r3.sm.extension.service.endpoint"
                     subscribedPrimaryType="alias_v6r3.sm.extension.service.endpoint"/>
   </rule-primary-types>
   <classification-filters>
      <ref-classification-filter name="sld-subscribable-govn-cf"/>
   </classification-filters>
   <relationship-filters>
      <relationship-filter appliesTo="ServiceLevelEntity"
         name="gep63_availableEndpoints"/>
   </relationship-filters>
</process-rule>
```

This process rule defines the processing of events that represent the transition of a Service Endpoint to an offline lifecycle state. If the event matches certain requirements, ITCAM for SOA deletes situations that were created for any policy attachments on any SLD with which the Service Endpoint is associated.

In the example event, the Service Endpoint is identified by the following attribute:

```
subscribedBsrUri="6dff3b6d-c31f-4f22.8c44.bfdeccbf4432"
```

The primary types determine that the process rule must be applied to SOAP, MQ, or Extension service endpoints:

```
   <rule-primary-types>
      <primary-types resourcePrimaryType="alias_v6r3.sm.soap.service.endpoint"
                     subscribedPrimaryType="alias_v6r3.sm.soap.service.endpoint"/>
      <primary-types resourcePrimaryType="alias_v6r3.sm.mq.service.endpoint"
                     subscribedPrimaryType="alias_v6r3.sm.mq.service.endpoint"/>
      <primary-types resourcePrimaryType="alias_v6r3.sm.extension.service.endpoint"
                     subscribedPrimaryType="alias_v6r3.sm.extension.service.endpoint"/>
   </rule-primary-types>
```

The action to take (delete situations) is determined by the following attribute:

```
operation="delete"
```

The following requirements must be met:

- The SLD must be in a subscribable state. This requirement is enforced by the `sld-subscribable-govn-cf` classification filter reference:

  ```
  <ref-classification-filter name="sld-subscribable-govn-cf"/>
  ```

- The SLD must be related to the service endpoint. This requirement is defined by the relationship filter for the `gep63_availableEndpoints` entity of the SLD.

  ```
  <relationship-filter appliesTo="ServiceLevelEntity"
      name="gep63_availableEndpoints">
  </relationship-filter>
  ```

Modifying the Process Rule

You might have to modify this process rule if WSRR has a custom governance enablement profile.

In this case, you must ensure that the following conditions are met:
- All the URIs in the process rule (including the classification filters that it references) are valid in the custom profile.
- The primary types section of the process rule lists all the valid service endpoint types.

Ensure that the URI of the WSRR lifecycle stage that triggers the process rule is correct in the following line:

```
transition="alias_v6r3.ld.revoke.from.use"
```

If the existing value of the alias does not match the value in the governance enablement profile, change the alias to the new value. Alternatively, use the new value in the process rule instead of the alias.

If new Service Endpoint types were added to the custom governance enablement profile, add them under the <rule-primary-types> tag, so that the process rule can include the new type when its checks the event.

To add a Service Endpoint type, you must know its classification URI. You can obtain it from the governance enablement profile. Then, add it to the primary types:

```
<rule-primary-types
  <primary-types resourcePrimaryType="alias_v6r3.sm.soap.service.endpoint"
    subscribedPrimaryType="alias_v6r3.sm.soap.service.endpoint"/>
  <primary-types resourcePrimaryType="alias_v6r3.sm.mq.service.endpoint"
    subscribedPrimaryType="alias_v6r3.sm.mq.service.endpoint"/>
  <primary-types resourcePrimaryType="alias_v6r3.sm.extension.service.endpoint"
    subscribedPrimaryType="alias_v6r3.sm.extension.service.endpoint"/>
  <primary-types resourcePrimaryType="<Service Endpoint classification URI>"
    subscribedPrimaryType="<Service Endpoint classification URI>"/>
</rule-primary-types>
```

You can also create an alias for the new Service Endpoint type, under the <aliases> tag:

```
alias name="new_se_type" value=<Service Endpoint classification URI>
```

Then you can reference the alias in the new <primary-types> tag:

```
  <primary-types resourcePrimaryType="alias_new_se_type"
    subscribedPrimaryType="alias_new_se_type"/>
```

If any Service Endpoint types are restricted in the custom governance profile, you can remove them from the rule primary types. For example, the following primary types definition means that only SOAP service endpoints trigger the process rule:

```
<rule-primary-types
  <primary-types resourcePrimaryType="alias_v6r3.sm.soap.service.endpoint
    subscribedPrimaryType="alias_v6r3.sm.soap.service.endpoint
</rule-primary-types>
```

Service Endpoint 'Remove Governance' Process Rule

The Service Endpoint 'Remove Governance' process rule determines the processing of the WSRR event that is generated when a Service Endpoint has its lifecycle governance removed in WSRR.

Overview

When ITCAM for SOA processes this event, it deletes situations that were created for any policy attachments on any SLD with which the Service Endpoint is associated.

Table 37 lists the processing of the WSRR event notification:

Table 37. ITCAM for SOA handling of removing governance from a service endpoint.

WSRR action	WSRR event	Event processing in ITCAM for SOA
Remove Governance	event=ˈREMOVE_GOVERNANCEˈ resourcePrimaryType= <Service Endpoint classification URI> subscribedPrimaryType= <Service Endpoint classification URI>	Process

WSRR Notification Event

When a Service Endpoint has its governance removed, WSRR sends an XML notification to ITCAM for SOA, as shown in the following example:

```
<?xml version="1.0" encoding="utf-8"?>
<body:resources xmlns:body="http://www.ibm.com/xmlns/prod/serviceregistry/
HttpPostNotifierPluginMsgBody">
  <body:resource bsrURI="f1dbd3f1-94a4-44b2.bd6a.639695636a6c"
     correlationId="correlation-id1"
     securityToken="security-token1"
     type="Subscription">
    <body:notificationResource event="REMOVE_GOVERNANCE"
        resourceBsrURI="6dff3b6d-c31f-4f22.8c44.bfdeccbf4432"
        resourceName="se_mq2"
        resourcePrimaryType="http://www.ibm.com/xmlns/prod/serviceregistry/
v6r3/ServiceModel#MQServiceEndpoint"
        resourceToSubscribedRelationship="sameObject"
        resourceType="GenericObject"
        subscribedBsrUri="6dff3b6d-c31f-4f22.8c44.bfdeccbf4432"
        subscribedName="se_mq2"
        subscribedPrimaryType="http://www.ibm.com/xmlns/prod/serviceregistry/
v6r3/ServiceModel#MQServiceEndpoint"
        subscribedType="GenericObject"/>
  </body:resource>
</body:resources>
```

Process Rule Definition

The default WSRR SDMS configuration file template includes the following process rule definition:

```
<!-- =======================================================
Service Endpoint ˈRemove Governanceˈ
======================================================= -->
<process-rule event="REMOVE_GOVERNANCE"
   represents="SLD_Relation_Governance"
   operation="delete"
   resourceToSubscribedRelationship="sameObject">
```

```
        <rule-primary-types>
          <primary-types resourcePrimaryType="alias_v6r3.sm.soap.service.endpoint"
                         subscribedPrimaryType="alias_v6r3.sm.soap.service.endpoint"/>
          <primary-types resourcePrimaryType="alias_v6r3.sm.mq.service.endpoint"
                         subscribedPrimaryType="alias_v6r3.sm.mq.service.endpoint"/>
          <primary-types resourcePrimaryType="alias_v6r3.sm.extension.service.endpoint"
                         subscribedPrimaryType="alias_v6r3.sm.extension.service.endpoint"/>
        </rule-primary-types>
        <classification-filters>
          <ref-classification-filter name="sld-subscribable-govn-cf"/>
        </classification-filters>
        <relationship-filters>
          <relationship-filter appliesTo="ServiceLevelEntity"
              name="gep63_availableEndpoints"/>
        </relationship-filters>
</process-rule>
```

This process rule defines the processing of events that represent the removal of governance from a Service Endpoint. If the event matches certain requirements, ITCAM for SOA deletes situations that were created for any policy attachments on any SLD with which the Service Endpoint is associated.

In the example event, the Service Endpoint is identified by the following attribute:

`subscribedBsrUri="6dff3b6d-c31f-4f22.8c44.bfdeccbf4432"`

The primary types determine that the process rule must be applied to SOAP, MQ, or Extension service endpoints:

```
    <rule-primary-types>
      <primary-types resourcePrimaryType="alias_v6r3.sm.soap.service.endpoint"
                     subscribedPrimaryType="alias_v6r3.sm.soap.service.endpoint"/>
      <primary-types resourcePrimaryType="alias_v6r3.sm.mq.service.endpoint"
                     subscribedPrimaryType="alias_v6r3.sm.mq.service.endpoint"/>
      <primary-types resourcePrimaryType="alias_v6r3.sm.extension.service.endpoint"
                     subscribedPrimaryType="alias_v6r3.sm.extension.service.endpoint"/>
    </rule-primary-types>
```

The action to take (delete situations) is determined by the following attribute:

`operation="delete"`

The following requirements must be met:

- The SLD must be in a subscribable state. This requirement is enforced by the classification filter reference `sld-subscribable-govn-cf`:

  `<ref-classification-filter name="sld-subscribable-govn-cf"/>`

- The SLD must be related to the service endpoint. This requirement is defined by the relationship filter for the `gep63_availableEndpoints` entity of the SLD.

  ```
  <relationship-filter appliesTo="ServiceLevelEntity"
      name="gep63_availableEndpoints">
  </relationship-filter>
  ```

Modifying the Process Rule

You might have to modify this process rule if WSRR has a custom governance enablement profile.

In this case, you must ensure that the primary types section of the process rule lists all the valid service endpoint types.

If new Service Endpoint types were added in the custom governance enablement profile, add them under the <rule-primary-types> tag, so that the process rule can include the new type when it checks the event.

To add a Service Endpoint type, you must know its classification URI. You can obtain it from the governance enablement profile. Then, add it to the primary types:

```
<rule-primary-types
  <primary-types resourcePrimaryType="alias_v6r3.sm.soap.service.endpoint"
    subscribedPrimaryType="alias_v6r3.sm.soap.service.endpoint"/>
  <primary-types resourcePrimaryType="alias_v6r3.sm.mq.service.endpoint"
    subscribedPrimaryType="alias_v6r3.sm.mq.service.endpoint"/>
  <primary-types resourcePrimaryType="alias_v6r3.sm.extension.service.endpoint"
    subscribedPrimaryType="alias_v6r3.sm.extension.service.endpoint"/>
  <primary-types resourcePrimaryType="<Service Endpoint classification URI>"
    subscribedPrimaryType="<Service Endpoint classification URI>"/>
</rule-primary-types>
```

You can also create an alias for the new Service Endpoint type, under the <aliases> tag:

```
alias name="new_se_type" value=<Service Endpoint classification URI>
```

Then, you can reference the alias in the new <primary-types> tag:

```
  <primary-types resourcePrimaryType="alias_new_se_type"
    subscribedPrimaryType="alias_new_se_type"/>
```

If any Service Endpoint types are restricted in the custom governance profile, you can remove them from the rule primary types. For example, the following primary types definition means that only SOAP service endpoints trigger the process rule:

```
<rule-primary-types
  <primary-types resourcePrimaryType="alias_v6r3.sm.soap.service.endpoint
    subscribedPrimaryType="alias_v6r3.sm.soap.service.endpoint
</rule-primary-types>
```

Service Endpoint 'Delete' Process Rule

The Service Endpoint 'Delete' process rule determines the processing of the WSRR event that is generated when a Service Endpoint is deleted in WSRR.

When ITCAM for SOA processes this event, it creates new situations or it updates or deletes exiting situations that were created for any policy attachments on any SLD with which the Service Endpoint is associated.

An SLD might be associated with one or more service endpoints. If the deleted service endpoint was one of several that are associated with the SLD, then the situation is updated in Tivoli Monitoring.

If the deleted service endpoint was the only one associated with the SLD, then the situation is deleted in Tivoli Monitoring.

If the deleted service endpoint was invalid and was one of several service endpoints associated with the SLD, a situation is created in Tivoli Monitoring, if all of the remaining service endpoints are valid.

Table 38 on page 101 lists the processing of the WSRR event notification:

Table 38. ITCAM for SOA processing of deleting a service endpoint.

WSRR action	WSRR event	Event processing in ITCAM for SOA
Service Endpoint Delete	event='DELETE' resourcePrimaryType= <Service Endpoint classification URI> subscribedPrimaryType= <Servioce Endpoint classification URI>	Process

WSRR Notification Event

When a Service Endpoint is deleted, WSRR sends an XML notification to ITCAM for SOA, as shown in the following example:

```
<?xml version="1.0" encoding="utf-8"?>
<body:resources xmlns:body="http://www.ibm.com/xmlns/prod/serviceregistry/
HttpPostNotifierPluginMsgBody">
  <body:resource bsrURI="f1dbd3f1-94a4-44b2.bd6a.639695636a6c"
      correlationId="correlation-id1"
      securityToken="security-token1"
      type="Subscription">
    <body:notificationResource event="DELETE"
        resourceBsrURI="6dff3b6d-c31f-4f22.8c44.bfdeccbf4432"
        resourceName="se_mq2"
        resourcePrimaryType="http://www.ibm.com/xmlns/prod/serviceregistry/
v6r3/ServiceModel#MQServiceEndpoint"
        resourceToSubscribedRelationship="sameObject"
        resourceType="GenericObject"
        subscribedBsrUri="6dff3b6d-c31f-4f22.8c44.bfdeccbf4432"
        subscribedName="se_mq2"
        subscribedPrimaryType="http://www.ibm.com/xmlns/prod/serviceregistry/
v6r3/ServiceModel#MQServiceEndpoint"
        subscribedType="GenericObject"/>
  </body:resource>
</body:resources>
```

Process Rule Definition

The default WSRR SDMS configuration file template includes the following process rule definition:

```
<!-- =========================================================
Service Endpoint 'Delete'
========================================================= -->
<process-rule event="DELETE"
   represents="SLD_Relation_Deletion"
   operation="createOrUpdate"
   resourceToSubscribedRelationship="sameObject">
   <rule-primary-types>
      <primary-types resourcePrimaryType="alias_v6r3.sm.soap.service.endpoint"
                     subscribedPrimaryType="alias_v6r3.sm.soap.service.endpoint"/>
      <primary-types resourcePrimaryType="alias_v6r3.sm.mq.service.endpoint"
                     subscribedPrimaryType="alias_v6r3.sm.mq.service.endpoint"/>
      <primary-types resourcePrimaryType="alias_v6r3.sm.extension.service.endpoint"
                     subscribedPrimaryType="alias_v6r3.sm.extension.service.endpoint"/>
   </rule-primary-types>
   <classification-filters>
      <ref-classification-filter name="sld-subscribable-govn-cf"/>
      <ref-classification-filter name="policy-expression-govn-cf"/>
   </classification-filters>
   <relationship-filters>
      <relationship-filter appliesTo="ServiceLevelEntity"
         name="gep63_availableEndpoints" ordinality="1">
         <ref-classification-filter name="service-endpoint-envr-cf"/>
```

```
            <ref-classification-filter name="service-endpoint-online-cf"/>
        </relationship-filter>
        <relationship-filter appliesTo="ServiceLevelEntity"
            name="gep63_availableOperations" ordinality="0">
            <ref-classification-filter name="service-operation-envr-cf"/>
            <ref-classification-filter name="service-operation-govn-cf"/>
        </relationship-filter>
    </relationship-filters>
</process-rule>
```

This process rule defines the processing of events that represent the deletion of a Service Endpoint. If the event matches certain requirements, ITCAM for SOA creates, updates, or deletes situations for any policy attachments on any SLD with which the Service Endpoint is associated.

In the example event, the Service Endpoint is identified by the following attribute:

`subscribedBsrUri="6dff3b6d-c31f-4f22.8c44.bfdeccbf4432"`

The primary types determine that the process rule must be applied to SOAP, MQ, or Extension service endpoints:

```
    <rule-primary-types>
        <primary-types resourcePrimaryType="alias_v6r3.sm.soap.service.endpoint"
                       subscribedPrimaryType="alias_v6r3.sm.soap.service.endpoint"/>
        <primary-types resourcePrimaryType="alias_v6r3.sm.mq.service.endpoint"
                       subscribedPrimaryType="alias_v6r3.sm.mq.service.endpoint"/>
        <primary-types resourcePrimaryType="alias_v6r3.sm.extension.service.endpoint"
                       subscribedPrimaryType="alias_v6r3.sm.extension.service.endpoint"/>
    </rule-primary-types>
```

The action to take (create, delete or update situations) is determined by the following attribute:

`operation="update"`

The following requirements must be met:

- The SLD must be in a subscribable state. This requirement is enforced by the `sld-subscribable-govn-cf` classification filter reference:

  `<ref-classification-filter name="sld-subscribable-govn-cf"/>`

- The SLD must have a policy attachment with the policy classification URI. This requirement is enforced by the `policy-expression-govn-cf` classification filter:

  `<ref-classification-filter name="policy-expression-govn-cf"/>`

- The SLD must have at least one service endpoint associated with it. This requirement is defined by the relationship filter for the `gep63_availableEndpoints` entity of the SLD. This filter also references classification filters to ensure that the service endpoint is online and in one of the monitored environments:

  ```
  <relationship-filter appliesTo="ServiceLevelEntity"
      name="gep63_availableEndpoints" ordinality="1">
    <ref-classification-filter name="service-endpoint-envr-cf"/>
    <ref-classification-filter name="service-endpoint-online-cf"/>
  </relationship-filter>
  ```

- The SLD can have zero or more service operations associated with it. This requirement is defined by the relationship filter for the `gep63_availableOperations` entity of the SLD. This filter references classification filters to ensure that any service operation can be monitored according to its lifecycle stage and is in one of the monitored environments:

```
    <relationship-filter appliesTo="ServiceLevelEntity"
        name="gep63_availableOperations" ordinality="0">
      <ref-classification-filter name="service-operation-envr-cf"/>
      <ref-classification-filter name="service-operation-govn-cf"/>
    </relationship-filter>
```

Modifying the Process Rule

You might have to modify this process rule if WSRR has a custom governance enablement profile.

In this case, you must ensure that the primary types section of the process rule lists all the valid service endpoint types.

If new Service Endpoint types were added to the custom governance enablement profile, add them under the <rule-primary-types> tag, so that the process rule can include the new type when its checks the event.

To add a Service Endpoint type, you must know its classification URI. You can obtain it from the governance enablement profile. Then, add it to the primary types:

```
<rule-primary-types
  <primary-types resourcePrimaryType="alias_v6r3.sm.soap.service.endpoint"
    subscribedPrimaryType="alias_v6r3.sm.soap.service.endpoint"/>
  <primary-types resourcePrimaryType="alias_v6r3.sm.mq.service.endpoint"
    subscribedPrimaryType="alias_v6r3.sm.mq.service.endpoint"/>
  <primary-types resourcePrimaryType="alias_v6r3.sm.extension.service.endpoint"
    subscribedPrimaryType="alias_v6r3.sm.extension.service.endpoint"/>
  <primary-types resourcePrimaryType="<Service Endpoint classification URI>"
    subscribedPrimaryType="<Service Endpoint classification URI>"/>
</rule-primary-types>
```

You can also create an alias for the new Service Endpoint type, under the <aliases> tag:

```
alias name="new_se_type" value=<Service Endpoint classification URI>
```

Then, you can reference the alias in the new <primary-types> tag:

```
  <primary-types resourcePrimaryType="alias_new_se_type"
    subscribedPrimaryType="alias_new_se_type"/>
```

If any Service Endpoint types are restricted in the custom governance profile, you can remove them from the rule primary types. For example, the following primary types definition means that only SOAP service endpoints trigger the process rule:

```
<rule-primary-types
  <primary-types resourcePrimaryType="alias_v6r3.sm.soap.service.endpoint
    subscribedPrimaryType="alias_v6r3.sm.soap.service.endpoint
</rule-primary-types>
```

Service Endpoint 'Update' Process Rule

The Service Endpoint 'Update' process rule determines the processing of the WSRR event that is generated when a Service Endpoint is edited in WSRR. The editing of properties, relationships or classifications for a Service Endpoint generates the event.

When ITCAM for SOA processes this event, it creates, updates, or deletes situations that were created for any policy attachments on any SLD with which the Service Endpoint is associated.

An SLD might be associated with one or more service endpoints. If the update in the service endpoint invalidates its relationship with an SLD, the situations that were created for that SLD are deleted.

If the update to the service endpoint creates a new relationship between an SLD and the service endpoint, situations for that SLD are created.

If the update to the service endpoint keeps an existing relationship between an SLD and the service endpoint, situations for that SLD are updated.

Table 39 lists the processing of the WSRR event notification:

Table 39. ITCAM for SOA processing of updating a service endpoint.

WSRR action	WSRR event	Event processing in ITCAM for SOA
Service Endpoint Update	event='UPDATE' resourcePrimaryType= <Service Endpoint classification URI> subscribedPrimaryType= <Service Endpoint classification URI>	Process

WSRR Notification Event

When a Service Endpoint is updated, WSRR sends an XML notification to ITCAM for SOA, as shown in the following example:

```
<?xml version="1.0" encoding="utf-8"?>
<body:resources xmlns:body="http://www.ibm.com/xmlns/prod/serviceregistry/
HttpPostNotifierPluginMsgBody">
  <body:resource bsrURI="f1dbd3f1-94a4-44b2.bd6a.639695636a6c"
    correlationId="correlation-id1"
    securityToken="security-token1"
    type="Subscription">
    <body:notificationResource event="UPDATE"
        resourceBsrURI="6dff3b6d-c31f-4f22.8c44.bfdeccbf4432"
        resourceName="se_mq2"
        resourcePrimaryType="http://www.ibm.com/xmlns/prod/serviceregistry/
v6r3/ServiceModel#MQServiceEndpoint"
        resourceToSubscribedRelationship="sameObject"
        resourceType="GenericObject"
        subscribedBsrUri="6dff3b6d-c31f-4f22.8c44.bfdeccbf4432"
        subscribedName="se_mq2"
        subscribedPrimaryType="http://www.ibm.com/xmlns/prod/serviceregistry/
v6r3/ServiceModel#MQServiceEndpoint"
        subscribedType="GenericObject"/>
  </body:resource>
</body:resources>
```

Process Rule Definition

The default WSRR SDMS configuration file template includes the following process rule definition:

```
<!-- =======================================================
Service Endpoint 'Update'
======================================================= -->
<process-rule event="UPDATE"
   represents="SLD_Relation_Update"
   startOn="createOrUpdate"
   operation="createOrUpdate"
   resourceToSubscribedRelationship="sameObject">
   <rule-primary-types>
```

```
        <primary-types resourcePrimaryType="alias_v6r3.sm.soap.service.endpoint"
                       subscribedPrimaryType="alias_v6r3.sm.soap.service.endpoint"/>
        <primary-types resourcePrimaryType="alias_v6r3.sm.mq.service.endpoint"
                       subscribedPrimaryType="alias_v6r3.sm.mq.service.endpoint"/>
        <primary-types resourcePrimaryType="alias_v6r3.sm.extension.service.endpoint"
                       subscribedPrimaryType="alias_v6r3.sm.extension.service.endpoint"/>
    </rule-primary-types>
    <classification-filters>
        <ref-classification-filter name="sld-subscribable-govn-cf"/>
        <ref-classification-filter name="policy-expression-govn-cf"/>
    </classification-filters>
    <relationship-filters>
        <relationship-filter appliesTo="ServiceLevelEntity"
            name="gep63_availableEndpoints" ordinality="1">
            <ref-classification-filter name="service-endpoint-envr-cf"/>
            <ref-classification-filter name="service-endpoint-online-cf"/>
        </relationship-filter>
        <relationship-filter appliesTo="ServiceLevelEntity"
            name="gep63_availableOperations" ordinality="0">
            <ref-classification-filter name="service-operation-envr-cf"/>
            <ref-classification-filter name="service-operation-govn-cf"/>
        </relationship-filter>
    </relationship-filters>
</process-rule>
```

This process rule defines the processing of events that represent the updating of a
Service Endpoint. If the event matches certain requirements, ITCAM for SOA
creates, deletes, or updates situations that were created for any policy attachments
on any SLD with which the Service Endpoint is associated.

In the example event, the Service Endpoint is identified by the following attribute:

```
subscribedBsrUri="6dff3b6d-c31f-4f22.8c44.bfdeccbf4432"
```

The primary types determine that the process rule must be applied to SOAP, MQ,
or Extension service endpoints:

```
    <rule-primary-types>
        <primary-types resourcePrimaryType="alias_v6r3.sm.soap.service.endpoint"
                       subscribedPrimaryType="alias_v6r3.sm.soap.service.endpoint"/>
        <primary-types resourcePrimaryType="alias_v6r3.sm.mq.service.endpoint"
                       subscribedPrimaryType="alias_v6r3.sm.mq.service.endpoint"/>
        <primary-types resourcePrimaryType="alias_v6r3.sm.extension.service.endpoint"
                       subscribedPrimaryType="alias_v6r3.sm.extension.service.endpoint"/>
    </rule-primary-types>
```

The action to take (create, delete, or update situations) is determined by the
combination of the following two attributes:

```
startOn="createOrUpdate"
operation="createOrUpdate"
```

The following requirements must be met:
- The SLD must be in a subscribable state. This requirement is enforced by the
  `sld-subscribable-govn-cf` classification filter reference:

  ```
  <ref-classification-filter name="sld-subscribable-govn-cf"/>
  ```
- The SLD must have a policy attachment with the policy classification URI. This
  requirement is enforced by the `policy-expression-govn-cf` classification filter:

  ```
  <ref-classification-filter name="policy-expression-govn-cf"/>
  ```
- The SLD must have at least one service endpoint associated with it. This
  requirement is defined by the relationship filter for the

gep63_availableEndpoints entity of the SLD. This filter also references classification filters to ensure that the service endpoint is online and in one of the monitored environments:

```
<relationship-filter appliesTo="ServiceLevelEntity"
    name="gep63_availableEndpoints" ordinality="1">
  <ref-classification-filter name="service-endpoint-envr-cf"/>
  <ref-classification-filter name="service-endpoint-online-cf"/>
</relationship-filter>
```

- The SLD can have zero or more service operations associated with it. This requirement is defined by the relationship filter for the gep63_availableOperations entity of the SLD. This filter references classification filters to ensure that any service operation can be monitored according to its lifecycle stage and is in one of the monitored environments:

```
<relationship-filter appliesTo="ServiceLevelEntity"
    name="gep63_availableOperations" ordinality="0">
  <ref-classification-filter name="service-operation-envr-cf"/>
  <ref-classification-filter name="service-operation-govn-cf"/>
</relationship-filter>
```

Modifying the Process Rule

You might have to modify this process rule if WSRR has a custom governance enablement profile.

In this case, you must ensure that the primary types section of the process rule lists all the valid service endpoint types.

If new Service Endpoint types were added in the custom governance enablement profile, add them under the <rule-primary-types> tag, so that the process rule can include the new type when its checks the event.

To add a Service Endpoint type, you must know its classification URI. You can obtain it from the governance enablement profile. Then, add it to the primary types:

```
<rule-primary-types
  <primary-types resourcePrimaryType="alias_v6r3.sm.soap.service.endpoint"
    subscribedPrimaryType="alias_v6r3.sm.soap.service.endpoint"/>
  <primary-types resourcePrimaryType="alias_v6r3.sm.mq.service.endpoint"
    subscribedPrimaryType="alias_v6r3.sm.mq.service.endpoint"/>
  <primary-types resourcePrimaryType="alias_v6r3.sm.extension.service.endpoint"
    subscribedPrimaryType="alias_v6r3.sm.extension.service.endpoint"/>
  <primary-types resourcePrimaryType="<Service Endpoint classification URI>"
    subscribedPrimaryType="<Service Endpoint classification URI>"/>
</rule-primary-types>
```

You can also create an alias for the new Service Endpoint type, under the <aliases> tag:

```
alias name="new_se_type" value=<Service Endpoint classification URI>
```

Then you can reference the alias in the new <primary-types> tag:

```
  <primary-types resourcePrimaryType="alias_new_se_type"
    subscribedPrimaryType="alias_new_se_type"/>
```

If any Service Endpoint types are restricted in the custom governance profile, you can remove them from the rule primary types. For example, the following primary types definition means that only SOAP service endpoints trigger the process rule:

```
<rule-primary-types
  <primary-types resourcePrimaryType="alias_v6r3.sm.soap.service.endpoint
    subscribedPrimaryType="alias_v6r3.sm.soap.service.endpoint
</rule-primary-types>
```

Service Operation 'Update' Process Rule

The Service Operation 'Update' process rule determines the processing of the WSRR event that is generated when a Service Operation is edited in WSRR. The editing of properties, relationships, or classifications for a Service Operation generates the event.

When ITCAM for SOA processes this event, it creates, updates, or deletes situations that were created for any policy attachments on any SLD with which the Service Operation is associated.

An SLD might be associated with zero or more service operations. If the update in the service operation invalidates its relationship with an SLD, the situations created for that SLD are be deleted.

If the update to the service operation creates a new relationship between an SLD and the service operation, situations for that SLD are created.

If the update to the service operation keeps an existing relationship between an SLD and the service operation, situations for that SLD are updated.

The following table lists the processing of the WSRR event notification:

Table 40. ITCAM for SOA processing of updating a service operation.

WSRR action	WSRR event	Event processing in ITCAM for SOA
Service Operation Update	event=`UPDATE` resourcePrimaryType= \<Service Operation classification URI> subscribedPrimaryType= \<Service Operation classification URI>	Process

WSRR Notification Event

When a Service Operation is updated, WSRR sends an XML notification to ITCAM for SOA, as shown in the following example:

```
<?xml version="1.0" encoding="utf-8"?>
<body:resources xmlns:body="http://www.ibm.com/xmlns/prod/serviceregistry/
HttpPostNotifierPluginMsgBody">
  <body:resource bsrURI="f1dbd3f1-94a4-44b2.bd6a.639695636a6c"
    correlationId="correlation-id1"
    securityToken="security-token1"
    type="Subscription">
    <body:notificationResource event="UPDATE"
        resourceBsrURI="610c8461-7a1c-4ca9.8f5f.041e6f045fa7"
        resourceName="validate"
        resourcePrimaryType="http://www.ibm.com/xmlns/prod/serviceregistry/
v6r3/ServiceModel#ServiceOperation"
        resourceToSubscribedRelationship="sameObject"
        resourceType="GenericObject"
        subscribedBsrUri="610c8461-7a1c-4ca9.8f5f.041e6f045fa7"
        subscribedName="validate"
        subscribedPrimaryType="http://www.ibm.com/xmlns/prod/serviceregistry/
```

```
v6r3/ServiceModel#ServiceOperation"
        subscribedType="GenericObject"/>
  </body:resource>
</body:resources>
```

Process Rule Definition

The default WSRR SDMS configuration file template includes the following process
rule definition:

```
<!-- =======================================================
Service Operation 'Update'
====================================================== -->
<process-rule event="UPDATE"
   represents="SLD_Relation_Update"
   startOn="createOrUpdate"
   operation="createOrUpdate"
   resourceToSubscribedRelationship="sameObject">
   <rule-primary-types>
      <primary-types resourcePrimaryType="alias_v6r3.sm.service.operation"
        subscribedPrimaryType="alias_v6r3.sm.service.operation"/>
   </rule-primary-types>
   <classification-filters>
      <ref-classification-filter name="sld-subscribable-govn-cf"/>
      <ref-classification-filter name="policy-expression-govn-cf"/>
   </classification-filters>
   <relationship-filters>
      <relationship-filter appliesTo="ServiceLevelEntity"
        name="gep63_availableEndpoints" ordinality="1">
        <ref-classification-filter name="service-endpoint-envr-cf"/>
        <ref-classification-filter name="service-endpoint-online-cf"/>
      </relationship-filter>
      <relationship-filter appliesTo="ServiceLevelEntity"
        name="gep63_availableOperations" ordinality="0">
        <ref-classification-filter name="service-operation-envr-cf"/>
        <ref-classification-filter name="service-operation-govn-cf"/>
      </relationship-filter>
   </relationship-filters>
</process-rule>
```

This process rule defines the processing of events that represent the updating of a
Service Operation. If the event matches certain requirements, ITCAM for SOA
creates, deletes, or updates situations that were created for any policy attachments
on any SLD with which the Service Operation is associated.

In the example event, the Service Operation is identified by the following attribute:

```
subscribedBsrUri="610c8461-7a1c-4ca9.8f5f.041e6f045fa7"
```

The primary types determine that the process rule must be applied to service
operations:

```
   <rule-primary-types>
      <primary-types resourcePrimaryType="alias_v6r3.sm.service.operation"
        subscribedPrimaryType="alias_v6r3.sm.service.operation"/>
   </rule-primary-types>
```

The action to take (create or update situations) is determined by the combination
of the following two attributes:

```
startOn="createOrUpdate"
operation="createOrUpdate"
```

The following requirements must be met:

- The SLD must be in a subscribable state. This requirement is enforced by the `sld-subscribable-govn-cf` classification filter reference:

```
<ref-classification-filter name="sld-subscribable-govn-cf"/>
```

- The SLD must have a policy attachment with the policy classification URI. This requirement is enforced by the `policy-expression-govn-cf` classification filter:

```
<ref-classification-filter name="policy-expression-govn-cf"/>
```

- The SLD must have at least one service endpoint associated with it. This requirement is defined by the relationship filter for the `gep63_availableEndpoints` entity of the SLD. This filter also references classification filters to ensure that the service endpoint is online and in one of the monitored environments:

```
<relationship-filter appliesTo="ServiceLevelEntity"
      name="gep63_availableEndpoints" ordinality="1">
   <ref-classification-filter name="service-endpoint-envr-cf"/>
   <ref-classification-filter name="service-endpoint-online-cf"/>
</relationship-filter>
```

- The SLD can have zero or more service operations associated with it. This requirement is defined by the relationship filter for the `gep63_availableOperations` entity of the SLD. This filter references classification filters to ensure that any service operation can be monitored according to its lifecycle stage and is in one of the monitored environments:

```
<relationship-filter appliesTo="ServiceLevelEntity"
      name="gep63_availableOperations" ordinality="0">
   <ref-classification-filter name="service-operation-envr-cf"/>
   <ref-classification-filter name="service-operation-govn-cf"/>
</relationship-filter>
```

Modifying the Process Rule

You might have to modify this process rule if WSRR has a custom governance enablement profile.

In this case, you must ensure that the primary types section of the process rule lists all the valid service operation types.

If new Service Operation types were added to the custom governance enablement profile, add them under the <rule-primary-types> tag, so that the process rule can include the new type when its checks the event.

To add a Service Endpoint type, you must know its classification URI. You can obtain it from the governance enablement profile. Then, add it to the primary types:

```
  <rule-primary-types>
     <primary-types resourcePrimaryType="alias_v6r3.sm.service.operation"
                            subscribedPrimaryType="alias_v6r3.sm.service.operation"/>
  <primary-types resourcePrimaryType="<Service Operation classification URI>"
    subscribedPrimaryType="<Service Operation classification URI>"/>
</rule-primary-types>
```

You can also create an alias for the new Service Endpoint type, under the <aliases> tag:

```
alias name="new_so_type" value=<Service Operation classification URI>
```

Then, you can reference the alias in the new <primary-types> tag:

```
  <primary-types resourcePrimaryType="alias_new_so_type"
    subscribedPrimaryType="alias_new_so_type"/>
```

Service Operation 'Delete' Process Rule

The Service Operation 'Delete' process rule determines the processing of the WSRR event that is generated when a service operation is deleted in WSRR. The deleting of a service operation generates an event.

When ITCAM for SOA processes this event, it resynchronizes, creates, or updates situations for any policy attachments on any SLD with which the service operation is associated.

An SLD may be associated with zero or more service operations.

If process rules are valid when the service operation is deleted, situations for the corresponding SLD are updated if they existed already, or created if they did not exist already.

The following table lists the processing of the WSRR event notification:

Table 41. ITCAM for SOA processing of updating a service operation.

WSRR action	WSRR event	Event processing in ITCAM for SOA
Service Operation Delete	event=`DELETE` resourcePrimaryType= `<Service Operation classification URI>`	Process

WSRR Notification Event

When a Service Operation is deleted, WSRR sends an XML notification to ITCAM for SOA, as shown in the following example:

```
<?xml version="1.0" encoding="utf-8"?>
<body:resources xmlns:body="http://www.ibm.com/xmlns/prod/serviceregistry/
HttpPostNotifierPluginMsgBody">
  <body:resource bsrURI="16998716-2b7e-4ec4.a7c0.94b32d94c041"
    correlationId="correlation-id1"
    securityToken="security-token1"
    type="Subscription">
    <body:notificationResource event="DELETE"
     resourceBsrURI="926bcb92-c5cd-4d30.b069.092f5e0969f1"
     resourceName="deleteTest"
            resourcePrimaryType="http://www.ibm.com/xmlns/prod/serviceregistry/
v6r3/ServiceModel#ServiceOperation"
            resourceToSubscribedRelationship="sameObject"
     resourceType="GenericObject"
     subscribedBsrUri="926bcb92-c5cd-4d30.b069.092f5e0969f1"
     subscribedName="deleteTest"
            subscribedPrimaryType="http://www.ibm.com/xmlns/prod/serviceregistry/
v6r3/ServiceModel#ServiceOperation"
            subscribedType="GenericObject"/>
  </body:resource>
</body:resources>
```

Process Rule Definition

The default WSRR SDMS configuration file template includes the following process rule definition:

```
<!-- ========================================================
Service Operation 'Delete'
========================================================= -->
<process-rule event="DELETE"
```

```
 operation="createOrUpdate"
 represents="SLD_Relation_Delete"
 resourceToSubscribedRelationship="sameObject">
 <rule-primary-types>
 <primary-types resourcePrimaryType="alias_v6r3.sm.service.operation"
subscribedPrimaryType="alias_v6r3.sm.service.operation"/>
  </rule-primary-types>

  <classification-filters>
  <ref-classification-filter name="sld-subscribable-govn-cf"/>
  <ref-classification-filter name="policy-expression-govn-cf"/>
  </classification-filters>

  <relationship-filters>

  <relationship-filter appliesTo="ServiceLevelEntity" name="gep63_availableEndpoints"
ordinality="1">
     <ref-classification-filter name="service-endpoint-envr-cf"/>
     <ref-classification-filter name="service-endpoint-online-cf"/>
  </relationship-filter>

  <relationship-filter appliesTo="ServiceLevelEntity" name="gep63_availableOperations"
ordinality="0">
     <ref-classification-filter name="service-operation-envr-cf"/>
     <ref-classification-filter name="service-operation-govn-cf"/>
  </relationship-filter>

  </relationship-filters>
</process-rule>
```

This process rule defines the processing of events that represent the deletion of a Service Operation. If the event matches certain requirements, ITCAM for SOA creates or updates situations that were created for any policy attachments on any SLD with which the Service Operation is associated.

In the example event, the Service Endpoint is identified by the following attribute:

```
subscribedBsrUri="926bcb92-c5cd-4d30.b069.092f5e0969f1"
```

The primary types determine that the process rule must be applied to service operations:

```
<rule-primary-types>
 <primary-types resourcePrimaryType="alias_v6r3.sm.service.operation"
subscribedPrimaryType="alias_v6r3.sm.service.operation"/>
</rule-primary-types>
```

The action to take (create or update situations) is determined by the combination of the following two attributes:

```
represents="SLD_Relation_Delete"
operation="createOrUpdate"
```

Important: To resynchronize situations, you must set the operation attribute to "resync".

The following requirements must be met:
- The SLD must be in a subscribable state. This requirement is enforced by the sld-subscribable-govn-cf classification filter reference:

  ```
  <ref-classification-filter name="sld-subscribable-govn-cf"/>
  ```
- The SLD must have a policy attachment with the policy classification URI. This requirement is enforced by the policy-expression-govn-cf classification filter:

  ```
  <ref-classification-filter name="policy-expression-govn-cf"/>
  ```

- The SLD must have at least one service endpoint associated with it. This requirement is defined by the relationship filter for the gep63_availableEndpoints entity of the SLD. This filter also references classification filters to ensure that the service endpoint is online and in one of the monitored environments:

```
<relationship-filter appliesTo="ServiceLevelEntity"
    name="gep63_availableEndpoints" ordinality="1">
  <ref-classification-filter name="service-endpoint-envr-cf"/>
  <ref-classification-filter name="service-endpoint-online-cf"/>
</relationship-filter>
```

- The SLD can have zero or more service operations associated with it. This requirement is defined by the relationship filter for the gep63_availableOperations entity of the SLD. This filter references classification filters to ensure that any service operation can be monitored according to its lifecycle stage and is in one of the monitored environments:

```
<relationship-filter appliesTo="ServiceLevelEntity"
    name="gep63_availableOperations" ordinality="0">
  <ref-classification-filter name="service-operation-envr-cf"/>
  <ref-classification-filter name="service-operation-govn-cf"/>
</relationship-filter>
```

Modifying the Process Rule

You might have to modify this process rule if WSRR has a custom governance enablement profile.

In this case, you must ensure that the primary types section of the process rule lists all the valid service operation types.

If new Service Operation types were added to the custom governance enablement profile, add them under the <rule-primary-types> tag, so that the process rule can include the new type when its checks the event.

To add a Service Operation type, you must know its classification URI. You can obtain it from the governance enablement profile. Then, add it to the primary types:

```
  <rule-primary-types>
     <primary-types resourcePrimaryType="alias_v6r3.sm.service.operation"
                          subscribedPrimaryType="alias_v6r3.sm.service.operation"/>
  <primary-types resourcePrimaryType="<Service Operation classification URI>"
    subscribedPrimaryType="<Service Operation classification URI>"/>
</rule-primary-types>
```

You can also create an alias for the new Service Endpoint type, under the <aliases> tag:

```
<alias name="new_so_type" value=<Service Operation classification URI>/>
```

You can reference the alias in the new <primary-types> tag:

```
  <primary-types resourcePrimaryType="alias_new_so_type"
    subscribedPrimaryType="alias_new_so_type"/>
```

SLD 'Resync' Process Rule

The SLD 'Resync' process rule determines the processing of the request for a resynchronization between WSRR and ITCAM for SOA.

The kd4WSRRITMSynchronization script (see Chapter 6, Synchronizing WSRR and ITCAM for SOA," on page 25) causes WSRR to send this event for every SLD.

When ITCAM for SOA processes this event, it creates, updates, or deletes situations depending on the properties, relationships, and classification of the SLD, SLM policy attachments, Service Endpoints and Service Operations in WSRR.

If an existing situation for an SLM policy that is attached to the SLD is invalid, SDMS deletes the situation.

If a situation for an SLM policy attached to the SLD does not exist, but must be created according to existing process rules, SDMS creates the situation.

If the properties or relationships related to a situation for an SLM policy that is attached to the SLD have to be updated, SDMS updates the situation.

Process Rule Definition

The default WSRR SDMS configuration file template includes the following process rule definition:

```
<!-- ========================================================
SLD 'Resync'
======================================================== -->
<process-rule event="RESYNC"
   represents="SLD_Resync">
   startOn="createOrUpdate">
   operation="resync">
   <classification-filters>
      <ref-classification-filter name="sld-subscribable-govn-cf"/>
      <ref-classification-filter name="policy-expression-govn-cf"/>
   </classification-filters>
   <relationship-filters>
      <relationship-filter appliesTo="ServiceLevelEntity"
         name="gep63_availableEndpoints" ordinality="1">
         <ref-classification-filter name="service-endpoint-envr-cf"/>
         <ref-classification-filter name="service-endpoint-online-cf"/>
      </relationship-filter>
      <relationship-filter appliesTo="ServiceLevelEntity"
         name="gep63_availableOperations" ordinality="0">
         <ref-classification-filter name="service-operation-envr-cf"/>
         <ref-classification-filter name="service-operation-govn-cf"/>
      </relationship-filter>
   </relationship-filters>
</process-rule>
```

This process rule defines the processing of events that represent a request for resynchronization. If the event matches certain requirements, ITCAM for SOA creates, deletes, or updates situations that were created for any SLM policy attached to the SLD.

The action to take (create and start situations) is determined by the combination of the following two attributes:

```
startOn="createOrUpdate">
operation="resync">
```

The following requirements must be met:
- The SLD must be in a subscribable state. This requirement is enforced by the `sld-subscribable-govn-cf` classification filter reference:

  ```
  <ref-classification-filter name="sld-subscribable-govn-cf"/>
  ```
- The SLD must have a policy attachment with the policy classification URI. This requirement is enforced by the `policy-expression-govn-cf` classification filter:

  ```
  <ref-classification-filter name="policy-expression-govn-cf"/>
  ```

- The SLD must have at least one service endpoint that is associated with it. This requirement is defined by the relationship filter for the gep63_availableEndpoints entity of the SLD. This filter also references classification filters to ensure that the service endpoint is online and in one of the monitored environments:

```
<relationship-filter appliesTo="ServiceLevelEntity"
    name="gep63_availableEndpoints" ordinality="1">
  <ref-classification-filter name="service-endpoint-envr-cf"/>
  <ref-classification-filter name="service-endpoint-online-cf"/>
</relationship-filter>
```

- The SLD can have zero or more service operations associated with it. This requirement is defined by the relationship filter for the gep63_availableOperations entity of the SLD. This filter references classification filters to ensure that any service operation can be monitored according to its lifecycle stage and is in one of the monitored environments:

```
<relationship-filter appliesTo="ServiceLevelEntity"
    name="gep63_availableOperations" ordinality="0">
  <ref-classification-filter name="service-operation-envr-cf"/>
  <ref-classification-filter name="service-operation-govn-cf"/>
</relationship-filter>
```

WSRR Notification Event and the Process Rule

Once a subscription has been established with a WSRR instance, ITCAM for SOA can consume and process WSRR notification events. These events determine if the process rules configured in ITCAM for SOA are triggered.

This is the general structure of a HTTP notification that WSRR sends to ITCAM for SOA. The values of the attributes have been left empty.

```
<?xml version="1.0" encoding="utf-8"?>
<body:resources xmlns:body="http://www.ibm.com/xmlns/prod/serviceregistry/
HttpPostNotifierPluginMsgBody">
  <body:resource bsrURI=""
      correlationId=""
      securityToken=""
      type="Subscription">
    <body:notificationResource event=""
        resourceBsrURI=""
        resourceName=""
        resourceToSubscribedRelationship=""
        resourceType=""
        subscribedBsrUri=""
        subscribedName=""
        subscribedPrimaryType=""
        subscribedType=""
        transition="">
      <policyUri></policyUri>
    </body:notificationResource>
  </body:resource>
</body:resources>
```

The attributes of the <body:resource> element relate to the subscription that was created in WSRR for ITCAM for SOA.

Table 42. <body:resource> attributes

Attribute	Value
bsrURI	The bsrURI of the subscription in WSRR. This value is displayed in the response from the kd4WSRRSubscriber command line tool.

Table 42. <body:resource> attributes (continued)

Attribute	Value
correlationId	The value specified in the `_correlationID` property in the subscription definition file.
securityToken	The value specified in the `_endPointSecurityToken` property in the subscription definition file.

The attributes of the <body:notificationResource> element relate to the action performed in WSRR. SDMS uses these attributes, as well as additional information on the WSRR entities (SLD, policy and so on) identified by these attributes, to determine if a process rule must be triggered.

The attributes are defined for two logical entities, the resource and the subscribed entity. What these entities represent is dependant on the context of the action in WSRR.

In the context of an SLD lifecycle transition or the editing of the SLD, the SLD is both the resource and the subscribed entity.

In the context of an SLM policy attach or detach, to or from an SLD, the resource is the policy and the subscribed entity is the SLD.

SDMS checks the attribute values in a process rule definition against attributes with the same name in <body:notificationResource>.

Table 43. <body:notificationResource> attributes and process rule definition attributes

Attribute	Value
event	The type of the WSRR event: TRANSITION, DELETE, UPDATE, ATTACH, DETACH, REMOVE_GOVERNANCE.
resourceToSubscribedRelationship	The relationship between the resource and the subscribed entity. If they are both the same, the value is `sameObject`. Otherwise, it defines the nature of the relationship, for example `attachedPolicy` if the resource is a policy attached to an SLD and subscribed entity is the SLD.
resourceType	The type of the resource entity, for example, `PolicyExpression` if the resource entity is an attached policy, or `GenericObject` if it is an SLD.
subscribedType	The type of the subscribed entity, for example, `PolicyExpression` if the resource entity is an attached policy, or `GenericObject` if it is an SLD.
transition	The URI of the governance lifecycle transition. This URI is determined by governance profile that is active in the WSRR instance.
resourcePrimaryType	The URI of the resource entity. This URI (for example, the classification URI of an SLD) is determined by the governance profile that is active in the WSRR instance.
subscribedPrimaryType	The URI of the subscribed entity. This URI (for example, the classification URI of an SLD) is determined by the governance profile that is active in the WSRR instance.

If the attributes of a <process-rule> match the attributes in the WSRR notification, WSRR evaluates the process rule further. It requests information for the resource and subscribed entities, and matches the classification and relationship filters in the process rule against the URIs in this information.

Chapter 8. Managing situations related to WSRR SLDs

When ITCAM for SOA receives a notification that an SLD in WSRR has become operational, it retrieves the SLD policy information from WSRR and automatically creates a situation for the SLD based on the process rules defined in the SDMS. A situation management script is provided to manage these situations.

About this task

Perform the following steps to run the situation management script.

Procedure

1. On the ITCAM for SOA host, change to the directory *KD4_DIR*/bin
2. Run the following command:
   - On Windows systems, kd4WSRRITMSituationMgmt.bat *arguments*
   - On Linux and UNIX systems, ./kd4WSRRITMSituationMgmt.sh *arguments*

   Use the following arguments. All arguments are required.

Table 44. Command line arguments for the situation management script

Command line arguments	Description
-sdmsHost *hostname*	The name of the Tivoli Enterprise Portal Server host
-sdmsPort *port*	The Tivoli Enterprise Portal Server HTTP transport port number. The default HTTP transport port number is 15210.
-sdmsUsername *username*	The IBM Tivoli Monitoring user name. This must be an IBM Tivoli Monitoring administrative user. You can use the user that has an alias in WSRR (see Creating an authentication alias for an IBM Tivoli Monitoring user˝ on page 6).
-sdmsPassword *password*	The IBM Tivoli Monitoring password for the user.
-wsrrInstances *instances*	The names of the WSRR instances, specified in the format [*wsrr_instance_1*,*wsrr_instance_2*]. The WSRR instance name must match the same string value as is used by the NAME attribute of the <wsrr_instance> tag under <wsrr_instances> in WSRR SDMS configuration file (see WSRR instances˝ on page 41. **Note:** The WSRR instances must be defined in the WSRR SDMS configuration file.
-operation *type*	The type of operation. The delete operation is the only option currently available. This operation removes all ITCAM for SOA situations created for all of the WSRR instances specified.

To determine the port number, see the HTTP transport port parameter in the following file on the Tivoli Enterprise Portal Server host:

- On Windows systems, *ITM_home*\CNPSJ\profiles\ITMProfile\logs\ AboutThisProfile.txt
- On Linux and UNIX systems, *ITM_home*/*architecture*/iw/profiles/ ITMProfile/logs/AboutThisProfile.txt

Examples

On a Windows system, the following command removes all situations relating to WSRR instance wsrr_instance_1.

```
kd4WSRRITMSituationMgmt.bat -operation delete -sdmsHost localhost -sdmsPort 15210
-sdmsUsername sysadmin -sdmsPassword sysadmin1 -wsrrInstances [wsrr_instance_1]
```

The following command on a Linux or UNIX system has the same effect:

```
./kd4WSRRITMSituationMgmt.sh -operation delete —sdmsHost localhost —sdmsPort 15210
   —sdmsUsername admin —sdmsPassword adminpassword -wsrrInstances [wsrr_instance_1]
```

On a Windows system, the following command removes all situations relating to WSRR instance wsrr_instance_1. Next, it removes all situations relating to WSRR instance wsrr_instance_2.

```
kd4WSRRITMSituationMgmt.bat -operation delete -sdmsHost localhost -sdmsPort 15210
-sdmsUsername sysadmin -sdmsPassword sysadmin1 -wsrrInstances [wsrr_instance_1,wsrr_instance_2]
```

The following command on a Linux or UNIX system has the same effect:

```
kd4WSRRITMSituationMgmt.sh -operation delete -sdmsHost localhost -sdmsPort 15210
-sdmsUsername sysadmin -sdmsPassword sysadmin1 -wsrrInstancess [wsrr_instance_1,wsrr_instance_2]
```

Chapter 9. Setting the tracing level

By default, SDMS logs every transaction that is received from WSRR, and logs information about the way it was processed. You can use this information to customize the WSRR SDMS configuration file. To conserve disk space and to optimize performance, you can change the tracing for the SDMS function to a higher level, for example, `warning` or `severe`.

About this task

The log files are located in the following directory:
- On Windows systems: *ITM_HOME*\CNPSJ\profiles\ITMProfile\logs\ITMServer
- On Linux and UNIX systems: *ITM_HOME*/*architecture*/iw/profiles/ITMProfile/logs/ITMServer

Complete the following procedure to change the tracing level:

Procedure

1. If the Tivoli Enterprise Portal Server administration console is disabled, enable it. For detail about enabling the administrative console, see the IBM Tivoli Monitoring information center at the URL:http://publib.boulder.ibm.com/infocenter/tivihelp/v15r1/topic/com.ibm.itm.doc_6.2.3/welcome.htm; search for Using the administration console˝.
2. Log in to the Tivoli Enterprise Portal Server administration console. The URL for this console is:

   `https://`*hostname*`:`*port*`/ibm/console/logon.jsp`

   hostname is the Tivoli Enterprise Portal Server host name.

   port is the Tivoli Enterprise Portal Server HTTPS transport port.

   To determine the port number, see the following file on the Tivoli Enterprise Portal Server host:
   - On Windows systems: *ITM_home*\CNPSJ\profiles\ITMProfile\logs\AboutThisProfile.txt
   - On Linux and UNIX systems: *ITM_home*/*architecture*/iw/profiles/ITMProfile/logs/AboutThisProfile.txt
3. Select **Troubleshooting** > **Logs and Trace**. The **Logging and Tracing** page opens.
4. In the server table, click the Tivoli Enterprise Portal Server name. The default name is **ITMServer**. The General Properties page opens.
5. Click **Change Log Detail Levels**.
6. Click the **Runtime** tab.
7. In the **Components** list, select the **com.ibm.management.soa.*** component. In the context menu, select **Messages and Trace Levels**, and choose the required trace level. The Groups text box contains the following string:

   `*=info: com.ibm.management.soa*=finer`

   Instead of `finer`, it contains the log level you have selected.

   The following log levels are available:
   - `fatal` (lowest level of logging)

- severe
- warning
- audit
- info (default level)
- config
- detail
- fine
- finer
- finest (highest level of logging)

8. Click **Apply**.

Chapter 10. Processing ITCAM for SOA situations in WSRR

ITCAM for SOA sends the name and creation time of the situations it automatically created to WSRR. This information is available from the policy attachment fields in WSRR. ITCAM for SOA also sends an event notification to WSRR when a situation is triggered or cleared. WSRR must process these events to inform its users of policy breaches. If you want WSRR to process ITCAM for SOA events, you must configure the WSRR Event Handler.

Situation information in WSRR policy attachments

When SDMS creates or modifies a situation for an SLD, WSRR places the situation information into the policy entity attached to the SLD. When SDMS deletes the situation, WSRR clears this information.

The following fields in the policy attachment contain ITCAM for SOA situation information:

Table 45. Policy attachment fields that contain ITCAM for SOA situation information

Field name	Content
itmSituationIdentifier	The name of the ITCAM for SOA situation.
itmSituationOwner	The IBM Tivoli Monitoring user that has created or modified this situation.
itmSituationTimestamp	The time when the situation was created.
itmSituationLastModified	The time when the situation was most recently modified.

Locating situation information in WSRR Policy attachment

ITCAM for SOA sends events to a WSRR Event Handler when a situation is triggered or cleared; the WSRR Event Handler places the situation information into the policy entity attached to the SLD. Once a situation has been triggered or cleared, you can verify that corresponding updates have been made to policy attachment in WSRR.

About this task

Perform the following steps to verify that, following the triggering of a situation in IBM Tivoli Monitoring, a policy entity attached to the SLD has been updated with situation information.

Procedure

1. Log in to **WSRR Web UI**.
2. From the **View** menu, select **Service Documents** -> **Policy Documents**.
3. Select a policy document.
4. On the Details page of the policy, click the **Policy** tab.
5. Select the **Policy Attachment**.
6. Select the **Policy** tab.

7. Verify that the situation properties have been added or updated by the Event Handler under **Additional properties**.

Configuring WSRR Event Handler to process situation events

ITCAM for SOA sends events to WSRR when a situation is triggered or cleared. If you want WSRR to process these events, you must configure the WSRR Event Handler.

About this task

Complete the following steps to configure the Event Handler.

For details about configuring the WSRR Event Handler, refer to WSRR information center at the URL: http://publib.boulder.ibm.com/infocenter/sr/v7r5/topic/com.ibm.sr.doc/twsr_configuringitcamforsoa.html.

Procedure

1. Log in to WSRR as a user with the configuration role assigned.
2. In the **Active Profile** menu, select **ITCAM Listener Integration**.
3. Select **ITCAMEventHandlerConfiguration**.
4. In the configuration field, for every situation that you want to process in WSRR, add XML content similar to the following example:

```
<TECEvent>
      <EventID>ResponseTimeWarning_610</EventID>
      <WSRRPropertyName compound="true">avg_elapsed_time_RTW_610
       </WSRRPropertyName>
      <WSRRReceivedPropertyValue>
        <StaticString>peak value</StaticString>
      </WSRRReceivedPropertyValue>
      <WSRRClearedPropertyValue>
        <StaticString>back to normal</StaticString>
      </WSRRClearedPropertyValue>
      <WSRRTargetType>Default</WSRRTargetType>
</TECEvent>
```

Supply the following information within the tags:

Table 46. Information in tags in the configuration field

Tag name	Content
<EventID>	The name of the ITCAM for SOA situation. You can copy this name from the `itmSituationIdentifier` field of the policy attachment. See Situation information in WSRR policy attachments" on page 121.
<WSRRPropertyName>	The name of the property that the Event Handler updates. This property belongs to the object that is determined by the content of the <WSRRTargetType> tag.
<WSRRReceivedPropertyValue>	The value to which the Event Handler sets the property when the situation is triggered.
<WSRRClearedPropertyValue>	The value to which the Event Handler sets the property when the situation is cleared.

Table 46. Information in tags in the configuration field (continued)

Tag name	Content
<WSRRTargetType>	The object that the Event Handler modifies. For the `Default` value, the Event Handler uses the service port name and service port namespace event properties to identify a WSDL Port or SCA Export object to update in the service registry. You can also set it to a value that results in the service endpoint being updated. For details about WSRR objects, see the WSRR information center. **Attention:** if you use the template WSRR SDMS configuration file, set the content of this tag to `Default`. Otherwise, the Event Handler modifies a service endpoint, and a service endpoint update triggers an ITCAM for SOA situation update. This creates an endless loop. If you have to configure the Event Handler to modify any service endpoint, remove the service endpoint update operation from the WSRR SDMS configuration file. Locate the comment "Service Endpoint `Update`" in the WSRR SDMS configuration file to identify the service endpoint update operation.

Locating situation information in WSRR metadata

ITCAM for SOA sends events to a WSRR Event Handler when a situation is triggered or cleared; the WSRR Event Handler updates metadata of a WSDL port or a SCA export by default, based on the event received. Once a situation has been triggered or cleared, you can verify that corresponding updates have been made to WSRR object properties.

About this task

Perform the following steps to verify that, following the triggering of a situation in IBM Tivoli Monitoring, an WSDL port or SCA export has been updated based on the mapping of situation event properties to WSRR object properties defined in the WSRR Event Handler.

Procedure
1. Log in to **WSRR Web UI**.
2. From the **View** menu, select **Service MetaData** -> **WSDL** -> **Ports**.
3. Select the service associated with the situation triggered.
4. Select **Custom properties** under **Additional properties**.
5. Verify that metadata properties have been added or updated by the Event Handler for the WSDLPort or SCA export object.

Chapter 11. Troubleshooting

You can encounter the following common problems when you are integrating ITCAM for SOA with WSRR or when you are using the integration.

Log size increasing too fast

The size of the log file (SystemOut.log) is constantly increasing.

By default, SDMS logs every transaction that is received from WSRR, and the way the transaction was processed. You can use the information in the log file to customize the WSRR SDMS configuration file.

If you do not need all of the log information, you can set the tracing for SDMS function to a higher level. For information about setting the tracing level, see Chapter 9, Setting the tracing level," on page 119.

A situation is not created, started, stopped, modified, or deleted on a WSRR notification

WSRR notifies ITCAM for SOA of a change (for example, an SLD has become subscribable) that requires ITCAM for SOA to create, start, stop, modify, or delete a situation, but ITCAM for SOA fails to complete the action.

You can use the following procedures to rectify the situation.

Checking the trace log for an operation classification URL

Check the trace log file for a message similar to the following text:

```
KD4DM0418I The target bsrUri [ca2ad5ca-9342-422f.a4e6.e2f764e2e61c] does not
match the classification filters for [ServiceOperation_Environment] on
relationship [gep63_availableOperations], returning invalid.
```

If this message is found, determine the service operation classification URL, and add it to the service-operation-envr-cf classification filter in the WSRR SDMS configuration file.

To determine the service operation classification URL, complete the following steps on the WSRR Web console:

1. Open the SLD.
2. On the **Details** tab, click the associated operation. WSRR displays detailed information about the service operation.
3. On the **Details** tab, click **Edit Classifications**.
4. From the **Classification** list, select the classification that applies to the service operation that is associated with the notification, for example, Scoped. WSRR displays the complete URL in the table displayed in the window.
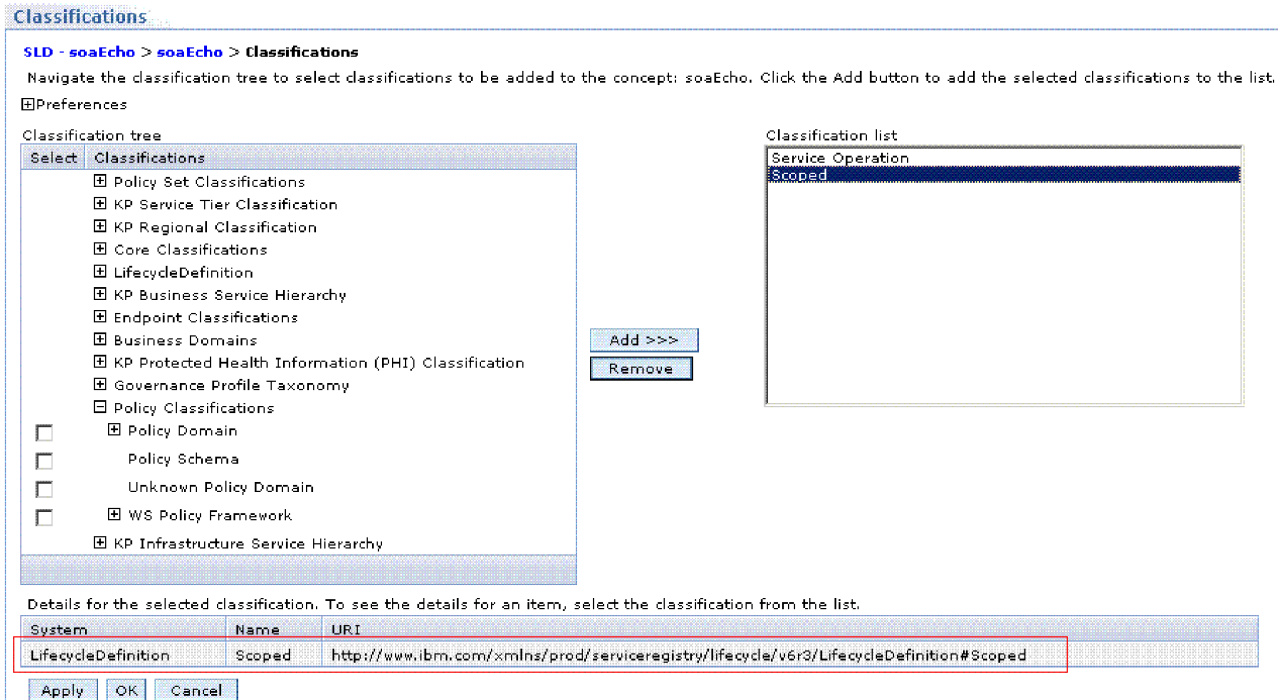
Figure 6. Viewing the service operation classification URL in WSRR

To add the URL, locate the classification filter named `service-operation-envr-cf`, and add a <classification> tag. Add the URL into the <classification> tag. For example:

```
<classification-filter-ref name="service-operation-envr-cf">
 <classification-filter appliesTo="ServiceOperation_Environment"
  uri="alias_v6r3.sm.service.operation">
   <classification uri="alias_v6r1.gp.taxonomy.production"/>
   <classification uri="alias_v6r1.gp.taxonomy.staging"/>
   <classification uri="alias_v6r1.gp.taxonomy.test"/>
   <classification uri="alias_v6r1.gp.taxonomy.development"/>
   <classification uri=
     "http://www.ibm.com/xmlns/prod/serviceregistry/lifecycle/v6r3/LifecycleDefinition#Scoped"/>
 </classification-filter>
</classification-filter-ref>
```

Checking the privileges of the Tivoli Monitoring user

Check the privileges of the IBM Tivoli Monitoring user specified in the SDMS configuration file. To check the privileges, complete the following steps:

1. Log on to the Tivoli Enterprise Portal console as a user with administrative rights.

2. From the main menu, select **Edit** > **Administer Users**.

3. On the Administer Users window, select the user that is configured in the WSRR SDMS configuration file.

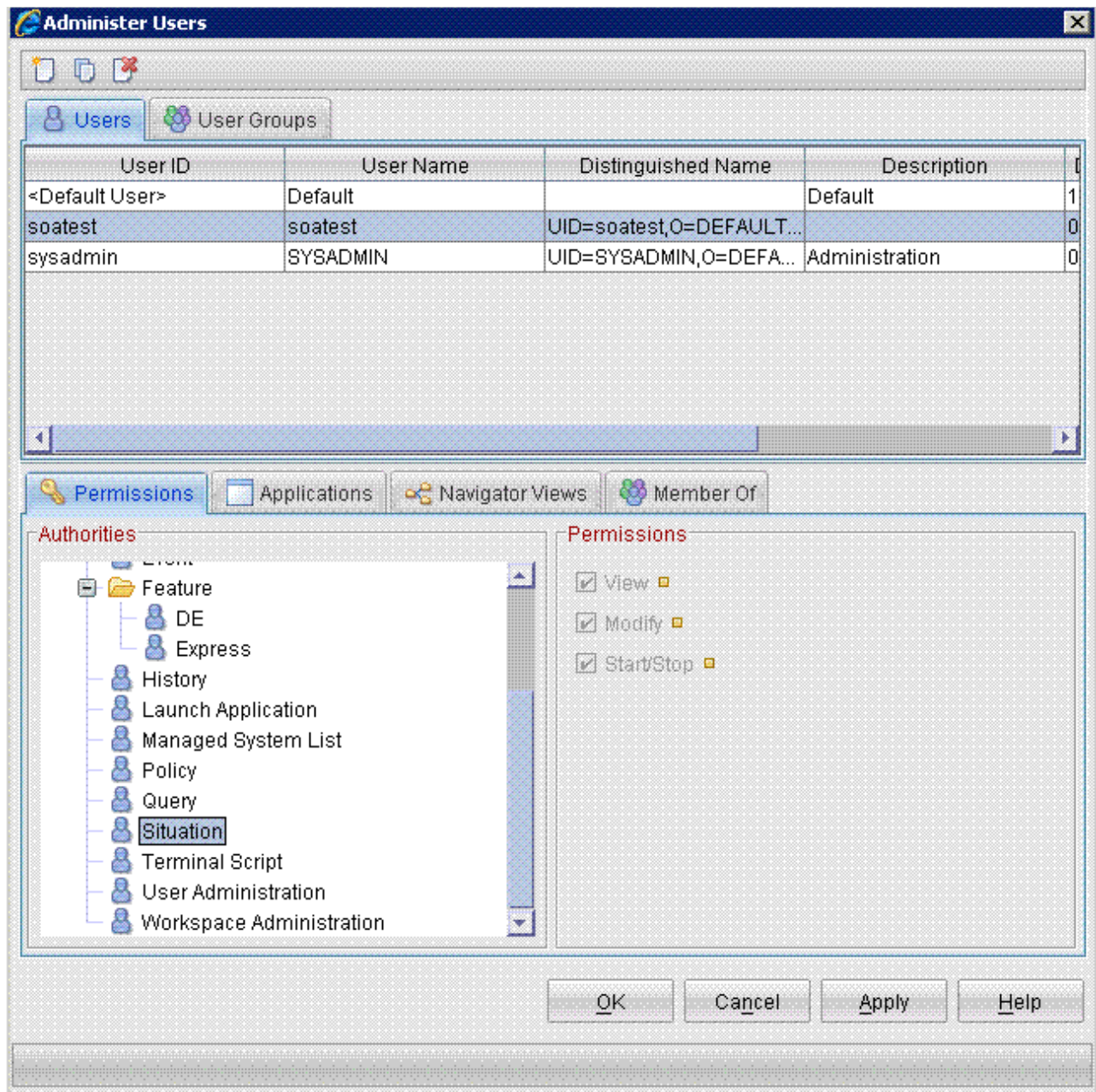4. Click the first tab **Permissions**. From the navigator tree, select **Situation**.

Figure 7. Viewing permissions for a Tivoli Monitoring user

5. All of the available permissions for a situation, **View**, **Modify**, and **Start/Stop**, must be available for the user. Otherwise, some or all situation changes that SDMS must complete cannot be completeed.

Checking the SLD and SLD-related entities in WSRR

Use the WSRR Web console to check for the following conditions. If any of the conditions is not true, modify the entity. For more information about the lifecycle of an SLD and related entities, see the WSRR information center at http://publib.boulder.ibm.com/infocenter/sr/v7r5/index.jsp.

- The SLD name must not include any double-byte characters. It must consist only of valid ASCII characters. (This is a limitation of the current version of WSRR).
- The SLD must be in the subscribable state.

- The policy that is attached to the SLD must be in the monitor state.
- Any service endpoints that are attached to the SLD must be in the online state.
- The classification URI of the SLD must be defined in the classification filters of the process rule.
- If the SLD has a service operation, the classification URI of the service must be defined in the classification filters of the process rule.

To determine the classification URI for an entity, see Checking the trace log for an operation classification URL" on page 125.

The trace log contains "Failed to execute the HTTP get"

The trace log contains a "Failed to execute the HTTP get" message, indicating that ITCAM for SOA cannot communicate correctly with WSRR.

About this task

To troubleshoot the connection problem, complete the following steps.

Procedure

1. Verify that the WSRR instance in the WSRR SDMS configuration file is defined correctly. Verify the host, port, username, password, and (when applicable) instance prefix attributes. See WSRR instances" on page 41.
2. Verify that the user has sufficient privileges in WSRR for querying and modifying policy information.
3. Locate the HTTP result code that is displayed in the log messages for more information on the error. ITCAM for SOA uses standard HTTP result codes, available at http://www.w3.org/Protocols/rfc2616/rfc2616-sec10.html. The following result codes are common:

   401 (Unauthorized)
   > If the log file includes this result code, the user name or password of the WSRR instance in the SDMS configuration file is incorrect, or the WSRR user does not have the required permissions. Ensure that you can log in to the WSRR with the user and password in the configuration file.

   404 (Not Found)
   > If the log file includes this result code, check that the WSRR instance details in the SDMS configuration file are correct, and that the WSRR server is reachable from the SDMS host. Using the SDMS host, ensure that you can log in to the WSRR with the user and password specified in the configuration file.

   407 (Proxy Authentication Required)
   > Check that the proxy configuration for the WSRR instance in the SDMS configuration file is correct, and that the proxy host can be reached from the SDMS host.

   408 (Timeout)
   > Check the availability and bandwidth of the connection between IBM Tivoli Monitoring and the WSRR instance.

A situation is not deleted when the SLD endpoint becomes invalid

SDMS creates situations for all monitored SLDs that are valid, and removes the situations when an SLD is no longer valid. However, if a service endpoint associated with an SLD becomes invalid, the existing situation is not deleted.

If this issue arises, you can delete the situation manually.

The issue is a limitation of the current version of ITCAM for SOA.

Appendix A. Accessibility

Accessibility features help users with physical disabilities, such as restricted mobility or limited vision, to use software products successfully.

The accessibility features in the product enable users to:

- Use assistive technologies, such as screen reader software and digital speech synthesizers, to hear what is displayed on the screen. Consult the product documentation of the assistive technology for details on using the technology with this product.
- Perform tasks with the software using only the keyboard.

General Navigation

Each page has four main sections:

- Headerbar
- Toolbar
- Main tabs
- Content

Each page has navigation points for screen readers. The following navigation points are all H1:

- Title bar
- Main tabs
- Main form
- Section labels
- Table labels

Menu Navigation

You use the Go To menu at the top of the screen to navigate to any of the applications that you have access to. The Go To menu is a cascading menu that is three levels deep at its deepest point. The following instructions describe how to get started with JAWS:

1. To get to the Go To menu press Alt+G.
2. When you open the menu, JAWS reads the first application in the menu. If JAWS does not begin to read the entry, restart the screen reader.
3. Navigate the list of applications in the menus by using the arrow keys.
4. JAWS indicates if a menu item has submenus. To get to a submenu, press the right arrow or enter.
5. Press the left arrow to move up a level in the hierarchy. If you press the left arrow at the highest level of the Go To menu, you leave the menu completely.
6. Press the Enter key to enter an application.

Accessibility help

The Accessibility Help panels provide details on general navigation, menu navigation, and hot keys. Click **Accessibility Help** from the toolbar of the product to access the help panels.

Screen reader setting

The product contains a screen reader flag. When you turn on the screen reader flag, the user interface is optimized to work with JAWS for Windows®. You use the **User** tab in the Users application to turn on the screen reader flag.

Keyboard shortcuts

You can navigate within the applications by using a combination of keys.

Accessible reports

To use the accessibility tools to read reports, you must access the reports in Microsoft Excel. In the reports applications, select the **Run Reports** option in the **Select Action** menu. With this option, you can email an .xls file version of a report to yourself at a scheduled time.

IBM and accessibility

For more information about the commitment that IBM has to accessibility, see the IBM Human Ability and Accessibility Center. The IBM Human Ability and Accessibility Center is at the following web address: http://www.ibm.com/able

Appendix B. Older version action types

In process rules, the attributes used to determine the action to take in IBM Tivoli Monitoring when an WSRR event notification is received have changed. This appendix provides the mapping between the older version attribute values and the new attributes values used in ITCAM for SOA version 7.2.

Attribute mapping

In ITCAM for SOA version 7.1.1 Fix Pack 3, the `represents` attribute in the <process_rule> tag of a process rule was used to indicate the situation-related action to take on receiving a specific type of WSRR event. In ITCAM for SOA version 7.2, to specify the process rule action, use a combination of `operation` and `startOn` attributes in the <process_rule> tag. To specific the specific WSRR event type on which to take the action, use the represents `attribute` in the <process_rule> tag.

The `operation` attribute specifies the situation-related operation to take on receiving the event notification from WSRR. The `startOn` attribute specifies whether to start the situation when a situation is created, updated or both. The `represents` attribute specifies the specific type of event from WSRR on which to apply the situation-related operation.

The following table presents a mapping of the values of the older version `represents` attribute to the new values of the `startOn`, `Operation`, and `represents` attributes:

Table 47. Mapping of the `represents` attribute values

Older version represents attribute	New startOn attribute	New operation attribute	New represents attribute
createSLDSituationsOnSETN	none	Create	SLD_Transition
createAndStartSLDSituationsOnSETN	create	start	SLD_Transition
deleteSLDSituationsOnSETN	none	delete	SLD_Delete
deleteSLDSituationsOnSERG	none	delete	SLD_Governance
stopSLDSituationsOnSETN	none	stop	SLD_Transition
startSLDSituationsOnSETN	create	create	SLD_Transition
createSLDSituationOnPolicyAttach	none	create	SLD_Policy_Attach
createAndStartSLDSituationOnPolicyAttach	create	create	SLD_Policy_Attach
deleteSLDSituationOnPolicyDetach	none	delete	SLD_Policy_Detach
resyncSLDSituations	none	resync	SLD_Resync
resyncAndStartSLDSituations	createOrUpdate	resync	SLD_Resync
updateSLDSituationOnPolicyUpdate	none	update	SLD_Policy_Update
createOrUpdateSLDSituationOnPolicyUpdate	none	createOrUpdate	SLD_Policy_Update
createAndStartOrUpdateSLDSituationOnPolicyUpdate	createOrUpdate	createOrUpdate	SLD_Policy_Update
deleteSLDSituationOnPERG	none	delete	SLD_Policy_Governance
createSLDSituationsOnRLTN	none	create	SLD_Relation_Transition
createAndStartSLDSituationsOnRLTN	create	create	SLD_Relation_Transition

Table 47. Mapping of the `represents` *attribute values (continued)*

Older version **represents attribute**	New **startOn** attribute	New operation attribute	New **represents attribute**
deleteSLDSituationsOnRLTN	none	delete	SLD_Relation_Transition
deleteSLDSituationsOnRLRG	none	delete	SLD_Relation_Governance
createSLDSituationOnPETN	none	create	SLD_Policy_Transition
createAndStartSLDSituationOnPETN	create	create	SLD_Policy_Transition
deleteSLDSituationOnPETN	none	delete	SLD_Policy_Transition
updateSLDSituationsOnSEUpdate	none	update	SLD_Update
createOrUpdateSLDSituationsOnSEUpdate	none	createOrUpdate	SLD_Update
createAndStartOrUpdateSLDSituationsOnSEUpdate	createOrUpdate	createOrUpdate	SLD_Update
updateSLDSituationsOnRLUpdate	none	update	SLD_Relation_Update
createOrUpdateSLDSituationsOnRLUpdate	none	createOrUpdate	SLD_Relation_Update
createAndStartOrUpdateSLDSituationsOnRLUpdate	createOrUpdate	createOrUpdate	SLD_Relation_Update
updateSLDSituationsOnRLDL	none	update	SLD_Relation_Deletion

Note: The older version `represents` attribute is still supported in Release 7.2 for backward compatability. However, you should migrate your process rules to use the new combination of `represents`, `startOn`, and `operation` attributes.

Process Rule Examples

The following example shows how the older version `represents` attribute was used prior to ITCAM for SOA version 7.2 in an SLD attach policy process rule to specify the action to take:

```
<process-rule event="ATTACH"
    represents="createAndStartSLDSituationOnPolicyAttach"
    resourceToSubscribedRelationship="attachedPolicy"
    resourceType="PolicyExpression">

    <rule-primary-types>
    <primary-types
     subscribedPrimaryType="alias_v6r3.gp.extensions.sld"/>
    <primary-types
     subscribedPrimaryType="alias_v6r3.ge.model.sld"/>
    </rule-primary-types>

    <classification-filters>
     <ref-classification-filter name="policy-expression-govncf"/>
     <ref-classification-filter name="sld-subscribable-govncf"/>
    </classification-filters>

    <relationship-filters>
     <relationship-filter appliesTo="ServiceLevelEntity"
     name="gep63_availableEndpoints" ordinality="1">
     <ref-classification-filter name="service-endpoint-envrcf"/>
     <ref-classification-filter name="service-endpointonline-
     cf"/>
     </relationship-filter>

     <relationship-filter appliesTo="ServiceLevelEntity"
     name="gep63_availableOperations" ordinality="0">
     <ref-classification-filter name="service-operationenvr-
     cf"/>
     <ref-classification-filter name="service-operationgovn-
```

```
      cf"/>
      </relationship-filter>
    </relationship-filters>
</process-rule>
```

The following example shows how a combination of the `represents, startOn` and `operation` attributes are used in ITCAM for SOA version 7.2 and later versions in the same SLD attach policy process rule to specify the action to take and the type of WSRR event on which to take the action:

```
<process-rule event="ATTACH"
    represents="SLD_Policy_Attach"
    startOn="create"
    operation="create"
    resourceToSubscribedRelationship="attachedPolicy"
    resourceType="PolicyExpression">

  <rule-primary-types>
   <primary-types
   subscribedPrimaryType="alias_v6r3.gp.extensions.sld"/>
   <primary-types subscribedPrimaryType="alias_v6r3.ge.model.sld"/>
  </rule-primary-types>

  <classification-filters>
   <ref-classification-filter name="policy-expression-govn-cf"/>
   <ref-classification-filter name="sld-subscribable-govn-cf"/>
  </classification-filters>

 <relationship-filters>
  <relationship-filter appliesTo="ServiceLevelEntity"
  name="gep63_availableEndpoints" ordinality="1">
   <ref-classification-filter name="service-endpoint-envr-cf"/>
   <ref-classification-filter name="service-endpoint-online-cf"/>
  </relationship-filter>

  <relationship-filter appliesTo="ServiceLevelEntity"
  name="gep63_availableOperations" ordinality="0">
   <ref-classification-filter name="service-operation-envr-cf"/>
   <ref-classification-filter name="service-operation-govn-cf"/>
  </relationship-filter>
 </relationship-filters>
</process-rule>
```

The following example shows how the older version `represents` attribute was used prior to ITCAM for SOA version 7.2 in an SLD detach policy process rule to specify the action to take and the type of WSRR event on which to take the action:

```
<process-rule event="DETACH"
   represents="deleteSLDSituationOnPolicyDetach"
   resourceToSubscribedRelationship="attachedPolicy"
   resourceType="PolicyExpression">
   <rule-primary-tyeps>
    <primary-types
     subscribedPrimaryType="alias_v6r3.gp.extensions.sld"/>
    <primary-types
     subscribedPrimaryType="alias_v6r3.ge.model.sld"/>
   </rule-primary-types>
</process-rule>
```

The following example shows how the older version `represents` attribute is used in ITCAM for SOA version 7.2 in the same SLD detach policy process rule to specify the action to take and the type of WSRR event on which to take the action:

```
<process-rule event="DETACH"
   represents="SLD_Policy_Detach"
   operation="delete"
```

```
resourceToSubscribedRelationship="attachedPolicy"
resourceType="PolicyExpression">
<rule-primary-types>
 <primary-types
 subscribedPrimaryType="alias_v6r3.gp.extensions.sld"/>
 <primary-types
 subscribedPrimaryType="alias_v6r3.ge.model.sld"/>
 </rule-primary-types>
</process-rule>
```

Note: The startOn attribute is optional and should only be used when a situation is being created or updated. If startOn is specified for a process rule that does not result in a situation being created or updated, the startOn attribute is ignored.

Index

A
accessibility   ix

B
books   vii

C
conventions
   typeface   x
cookies   142

D
directories, variables for   xi

E
education
   See Tivoli technical training

I
ITM_home   xi

K
KD4_DIR   xi

M
manuals   vii

O
ordering publications   ix

P
privacy policy   142
publications   vii
   ordering   ix

R
reader requirements   vii
requirements for readers   vii

S
service   x
service management connect   x
SMC   x
support   x

T
Tivoli technical training   x
Tivoli user groups   x
training, Tivoli technical   x
typeface conventions   x

U
user groups, Tivoli   x

V
variables for directories   xi

Trademarks

IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the web at Copyright and trademark information˝ at http://www.ibm.com/legal/copytrade.shtml.

Adobe and all Adobe-based trademarks are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States, other countries, or both.

Linux is a trademark of Linus Torvalds in the United States, other countries, or both.

Microsoft and Windows are trademarks of Microsoft Corporation in the United States, other countries, or both.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Java and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.

Notices

This information was developed for products and services offered in the U.S.A. IBM might not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM might have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785 U.S.A.

For license inquiries regarding double-byte (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan, Ltd.
19-21, Nihonbashi-Hakozakicho, Chuo-ku
Tokyo 103-8510, Japan

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law:

INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY FITNESS FOR A PARTICULAR PURPOSE.

Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement might not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements or changes in the product(s) or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who want to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Corporation
2Z4A/101
11400 Burnet Road
Austin, TX   78758   U.S.A.

Such information might be available, subject to appropriate terms and conditions, including in some cases payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement or any equivalent agreement between us.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments might vary significantly. Some measurements might have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurement might have been estimated through extrapolation. Actual results might vary. Users of this document should verify the applicable data for their specific environment.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. You may copy, modify, and distribute these sample programs in any form without payment to IBM for the purposes of developing, using, marketing, or distributing application programs conforming to IBMs application programming interfaces.

Privacy policy considerations

IBM Software products, including software as a service solutions, (Software Offerings˝) may use cookies or other technologies to collect product usage information, to help improve the end user experience, to tailor interactions with the end user or for other purposes. In many cases no personally identifiable

information is collected by the Software Offerings. Some of our Software Offerings can help enable you to collect personally identifiable information. If this Software Offering uses cookies to collect personally identifiable information, specific information about this offering˙s use of cookies is set forth below.

Depending upon the configurations deployed, this Software Offering may use session cookies that collect each user˙s user name for purposes of session management, authentication, and single sign-on configuration. These cookies cannot be disabled.

If the configurations deployed for this Software Offering provide you as customer the ability to collect personally identifiable information from end users via cookies and other technologies, you should seek your own legal advice about any laws applicable to such data collection, including any requirements for notice and consent.

For more information about the use of various technologies, including cookies, for these purposes, See IBM˙s Privacy Policy at http://www.ibm.com/privacy and IBM˙s Online Privacy Statement at http://www.ibm.com/privacy/details the section entitled Cookies, Web Beacons and Other Technologies˝ and the IBM Software Products and Software-as-a-Service Privacy Statement˝ at http://www.ibm.com/software/info/product-privacy.

IBM ®

Printed in USA