Oracle® Enterprise Manager

Installation and Configuration Guide for Microsoft Systems Center Operations Manager Connector

Release 12.1 (1.0.5.2.0)

E14736-07

May 2011

ORACLE®

Oracle Enterprise Manager Installation and Configuration Guide for Microsoft Systems Center Operations Manager Connector, Release 12.1 (1.0.5.2.0)

E14736-07

Primary Author: Michael Zampiceni

Contents

3 Configuring the Connector

4 Changing Default Configurations

5 Troubleshooting the Connector

A Default Mappings

Index

Preface

This *Installation and Configuration Guide for Microsoft Systems Center Operations Manager (SCOM) Connector* provides the required information to install and configure the Microsoft System Center Operations Manager (SCOM) Connector that integrates Oracle Enterprise Manager with SCOM management tools and help desk systems.

Audience

This guide is written for Oracle Enterprise Manager system administrators who want to install and configure the Microsoft SCOM Connector to enable integration between Oracle Enterprise Manager and Microsoft SCOM.

You should already be familiar with Oracle Enterprise Manager.

Documentation Accessibility

Our goal is to make Oracle products, services, and supporting documentation accessible to all users, including users that are disabled. To that end, our documentation includes features that make information available to users of assistive technology. This documentation is available in HTML format, and contains markup to facilitate access by the disabled community. Accessibility standards will continue to evolve over time, and Oracle is actively engaged with other market-leading technology vendors to address technical obstacles so that our documentation can be accessible to all of our customers. For more information, visit the Oracle Accessibility Program Web site at

`http://www.oracle.com/accessibility/`

Accessibility of Code Examples in Documentation

Screen readers may not always correctly read the code examples in this document. The conventions for writing code require that closing braces should appear on an otherwise empty line; however, some screen readers may not always read a line of text that consists solely of a bracket or brace.

Accessibility of Links to External Web Sites in Documentation

This documentation may contain links to Web sites of other companies or organizations that Oracle does not own or control. Oracle neither evaluates nor makes any representations regarding the accessibility of these Web sites.

TTY Access to Oracle Support Services

To reach Oracle Support Services, use a telecommunications relay service (TRS) to call Oracle Support at 1.800.223.1711.

Related Documents

For more information, see the following books in the Oracle Enterprise Manager documentation set:

- *Oracle Enterprise Manager Connectors Integration Guide*
- *Oracle Database 2 Day DBA*
- *Oracle Enterprise Manager Concepts*
- *Oracle Enterprise Manager Quick Installation Guide*
- *Oracle Enterprise Manager Grid Control Installation and Basic Configuration*
- *Oracle Enterprise Manager Advanced Configuration*
- *Oracle Enterprise Manager Metric Reference Manual*
- *Oracle Enterprise Manager Command Line Interface*
- *Extending Oracle Enterprise Manager*

The latest versions of this and other Oracle Enterprise Manager documentation can be found at:

`http://www.oracle.com/technology/documentation/oem.html`

Oracle Enterprise Manager also provides extensive online help. Click **Help** on any Oracle Enterprise Manager page to display the online Help system.

Printed documentation is available for sale in the Oracle Store at

`http://oraclestore.oracle.com/`

To download free release notes, installation documentation, white papers, or other collateral, please visit the Oracle Technology Network (OTN). You must register online before using OTN; registration is free and can be done at

`http://otn.oracle.com/membership/`

If you already have a user name and password for OTN, then you can go directly to the documentation section of the OTN Web site at

`http://otn.oracle.com/documentation/`

Conventions

The following text conventions are used in this document:

Convention	Meaning
boldface	Boldface type indicates graphical user interface elements associated with an action, or terms defined in text or the glossary.
italic	Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.
`monospace`	Monospace type indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that you enter.

1

Introduction and Requirements

The Microsoft Systems Center Operations Manager (SCOM) Connector (version 1.0.5.1.0) integrates Oracle Enterprise Manager with Microsoft SCOM 2007 through web services, enabling you to exchange alert information between the two systems.

1.1 Connector Features

The Oracle Management Connector for Microsoft SCOM enables you to forward Enterprise Manager alerts to SCOM and receive Enterprise Manager alerts raised by SCOM. This ensures that the two systems are always synchronized, providing administrators with current information about their entire data center.

The connector supports the following features:

- Synchronization of the alert life cycle on both ends
- Customization of alert mappings during the alert information exchange
- Bi-directional flow of alert information

  The connector reflects the change in alert severity as the severity changes in the alert originating system. For example, if an alert is forwarded from Oracle Enterprise Manager to SCOM, all the state changes in Enterprise Manager are reflected in SCOM. However, if you change the state of the alert in SCOM, the change is not reflected in Enterprise Manager because the alert originated in Enterprise Manager. This is also the case for the other direction.

The following sections explain how the connector handles SCOM alerts and polls the SCOM web service.

1.2 Oracle Enterprise Manager Alerts Transmitted to SCOM Events

Whenever an alert is triggered in Oracle Enterprise Manager, the SCOM Connector can automatically create or update an alert in SCOM. You can use Notification Rules to specify the set of alerts for which alerts must be created, and the alert severity for which this should happen.

After the connector creates an alert in SCOM, any subsequent change of the alert severity is propagated to Microsoft SCOM. When the severity of the alert changes to Clear in Oracle Enterprise Manager, the corresponding alert is closed in SCOM.

Figure 1–1 shows an example of an Oracle Enterprise Manager alert.

Figure 1–1 Oracle Enterprise Manager Alert

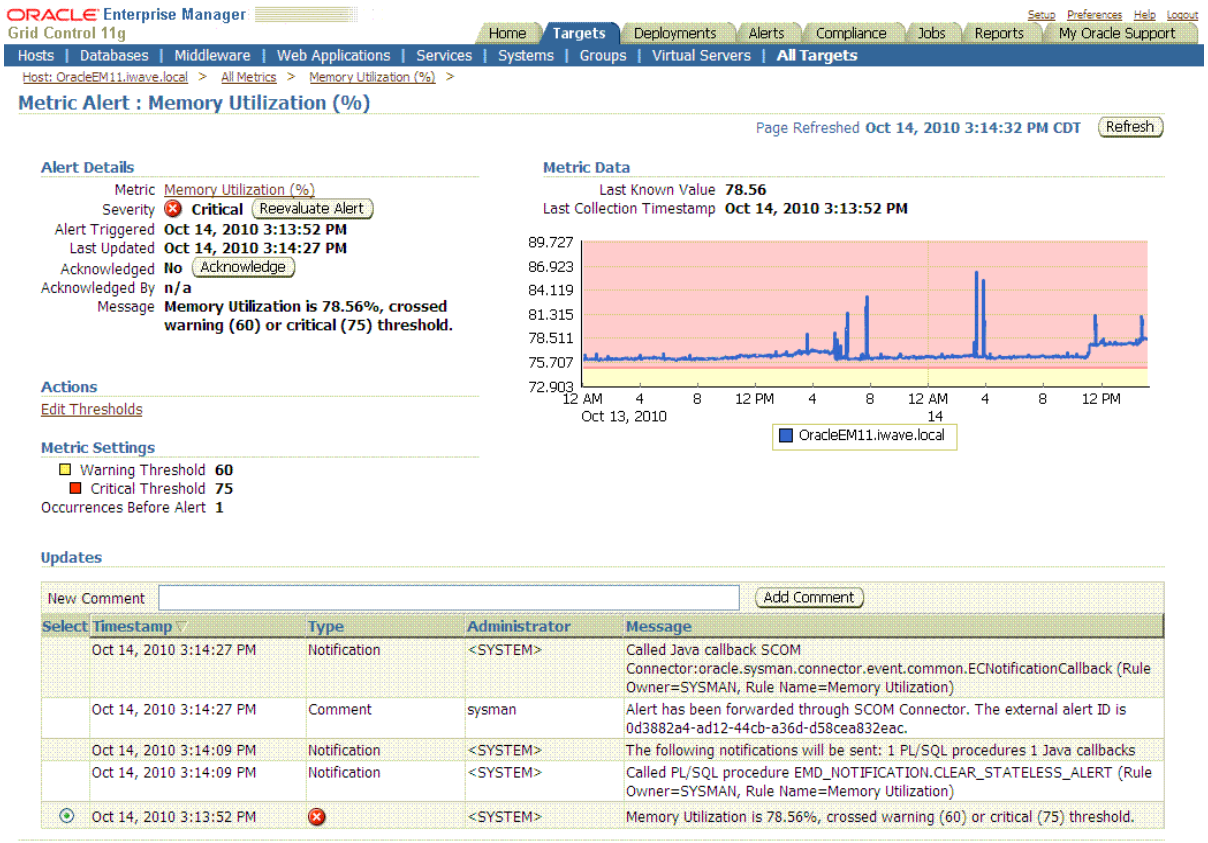
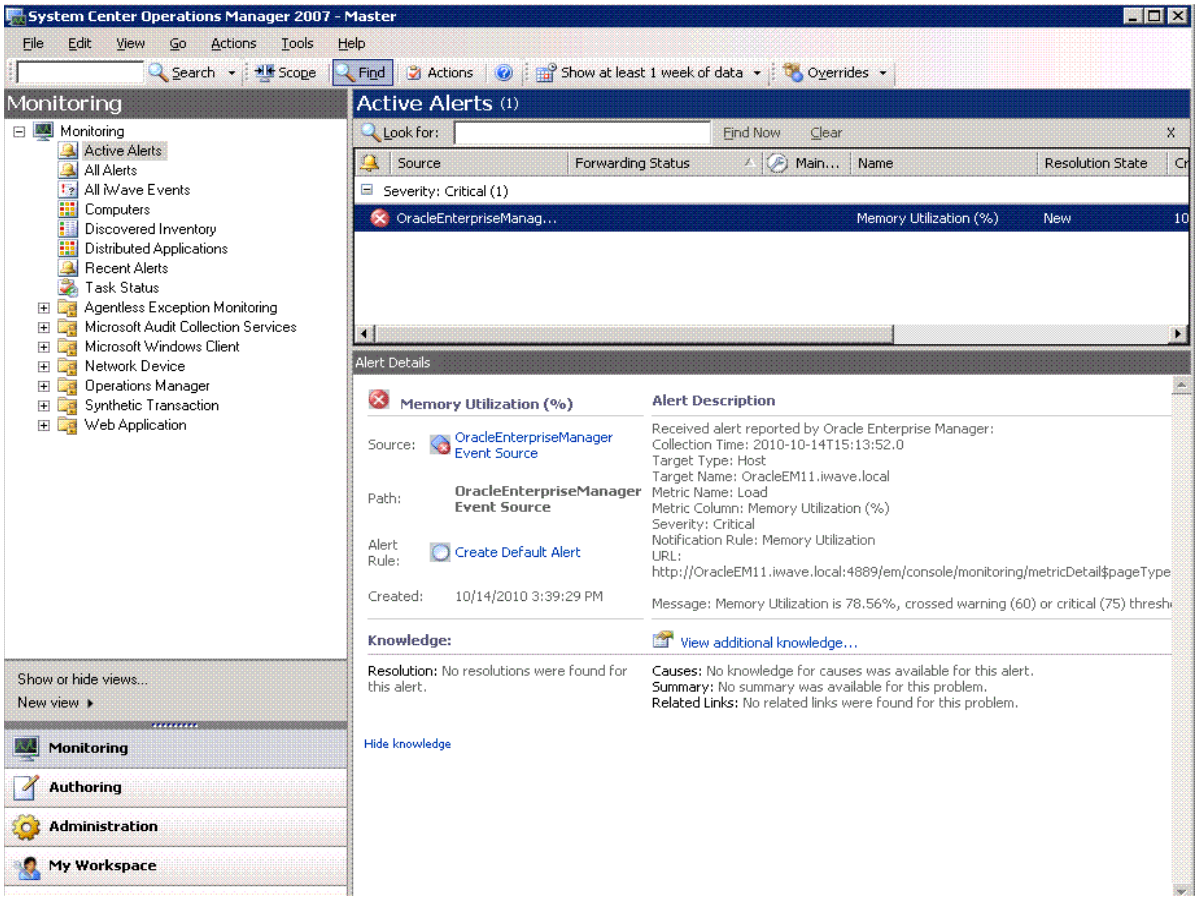


Figure 1–2 shows an example of a Microsoft SCOM alert.

Figure 1–2 Microsoft SCOM Alert



1.3 Versions Supported

This connector supports the following versions of Oracle Enterprise Manager and Microsoft SCOM:

- Oracle Enterprise Manager Grid Control 10g Release 5 with one-off patch # 8228087
- Oracle Enterprise Manager Grid Control 11g Release 1
- Microsoft Systems Center Operations Manager version 2007 (including R2)

You can install the SCOM Agent on the Microsoft Windows (2000, 2003, XP) platform.

The base Enterprise Manager version number for the Microsoft Systems Center Operations Manager Connector Release 1.0.5.1.0 is Enterprise Manager 10*g* Release 5.

1.4 Prerequisites

Before using the Microsoft SCOM connector, ensure that you meet the following prerequisites:

- For only Grid Control 10g Release 5, download the following Oracle Patch:
  1. Download one-off patch # 8228087 from My Oracle Support at:

     `http://metalink.oracle.com/`

2. Follow the instructions included with the download in the `README.txt` file.

- A utility for unzipping `.zip` files is available where the SCOM Agent is to be installed.
- Java JRE 6.0 or higher is installed on the system where the SCOM Web Service will be installed.

If you want Oracle Enterprise Manager to forward alerts to Microsoft SCOM, you need to import the OracleEnterpriseManager.Alert.Creator Management Pack from the Microsoft SCOM server. The Management Pack file is provided with the SCOM Agent installation binaries.

2

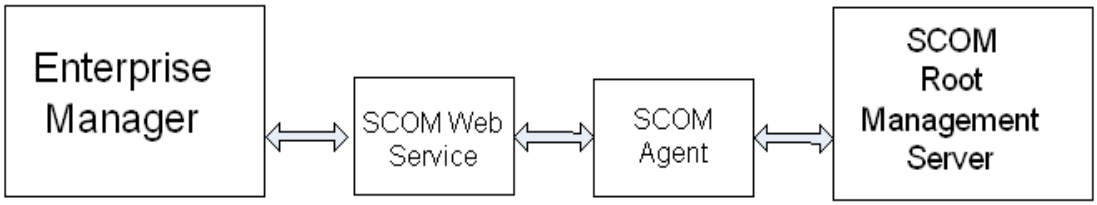
Installing the Connector

The Oracle Enterprise Manager Connector Framework requires a web service interface for exchanging event information with Microsoft SCOM. To integrate with Enterprise Manager, a third-party SCOM web service front-end must be installed. In addition to the web service front-end, an Oracle SCOM Agent must also be installed. Both of these components are included in the Oracle Enterprise Manager installation package.

You can install the web service on any Unix or Windows system that has connectivity with the SCOM server. In addition to the SCOM web service front-end, you must also install a back-end SCOM Agent. The Oracle SCOM Agent is preconfigured and is also included in the Oracle Enterprise Manager installation package.

Figure 2–1 shows the communication between the various components of the SCOM Connector.

Figure 2–1 Connector Communication Between Components



The following sections in this chapter discuss these topics:

- Installation Platforms
- Installing and Running the Oracle SCOM Agent
- Installing the Microsoft SCOM Web Service
- Installing the Microsoft SCOM Connector in Oracle Enterprise Manager
- Registering Templates

2.1 Installation Platforms

You can install the SCOM web service on the following platforms that support Java JRE 1.6:

- Microsoft Windows
- Sun Solaris

- HP-UX
- Linux

You can install the Oracle SCOM Agent on the Microsoft Windows (2000, 2003, 2008, XP) platform.

2.2 Installing and Running the Oracle SCOM Agent

The following sections provide procedures for installing and running the Oracle SCOM Agent.

2.2.1 Preinstallation Requirements

The following requirements apply to the system where the Oracle SCOM Agent is installed.

- .NET framework 2.0 is installed
- .NET framework 3.0 is installed
- ASP.NET 2.0 is installed

  After .NET frameword 2.0 is installed, enter the following command to install ASP.NET 2.0:

  ```
  %SystemRoot%\Microsoft.NET\Framework\v2.0.xxxxx\aspnet_regiis -i
  ```

  WARNING: This command upgrades other applications running under IIS to version 2.0.

- Internet Information Services (IIS) 5.0 or higher is installed
- Operations Manager 2007 Console is installed
- ASP.NET 2.0 extensions are enabled in IIS

  WARNING: Before proceeding, enabling ASP.NET 2.0 extensions may affect other applications that are running under IIS in an earlier version.

  To enable ASP.NET extensions, perform the following steps:

  1. Open the IIS Manager and expand the local computer in the left pane.
  2. Right-click on Web Service Extensions and select **Allow all Web service extensions for a specific application …**
  3. Select **ASP.NET v2.0.0xxxxx** from the pull-down list, where xxxxx is the version of the .NET framework 2.0 that is installed.
  4. Click **OK** to enable the ASP.NET extensions.

2.2.2 Setting Up the Agent Account

Before installing the Oracle SCOM Agent, you need to set up an account for the Oracle SCOM Agent to access the SCOM API. The account must satisfy the following requirements:

- Must be a domain account

- Must be used exclusively by the Oracle SCOM Agent
- Must have local administrator permissions
- Must be a member of a group designated as an Ops Mgr Administrator (See "Ops Mgr Administrator Groups" below)
- Must be a member of an Ops Mgr role that has an Author profile (See "Ops Mgr user role for Oracle SCOM Agent" below)

Ops Mgr Administrator Groups

To determine the groups that are designated as an Ops Mgr Administrator, perform the following steps:

1. In the Administration pane of the Ops Mgr 2007 console, select **Administration**, then **Security**, then **User Roles**. The User Roles should be displayed in the center pane.
2. Right-click on Operations Manager Administrators and select **Properties**. The General tab lists the groups that have administrative permissions in the User Role members window. The account the Agent uses must be a member of one of the groups listed here, or you need to add one of its groups to this list.

Ops Mgr user role for Oracle SCOM Agent

To add a new Ops Mgr 2007 user role for the Oracle SCOM Agent, perform the following steps:

1. In the Administration pane of the Ops Mgr 2007 console, select **Administration**, then **Security**, then **User Roles**. Right-click on **User Roles** and select **New User Role**, then **Author**. The Create User Role wizard window appears.
2. Enter the name of the Oracle SCOM Agent in the **User Role Name** field.
3. Click **Add** to add a user role member. The Select Users or Groups pop-up window appears.
4. Enter the domain user account information in the **Enter the object names to select** dialog box.

   Since this is a domain user account, you need to specify the account as <DOMAIN>\<username> , where <DOMAIN> is the Windows domain where the account was created, and <username> is the user name of the account set up for the Oracle SCOM Agent.
5. Click **OK** to add the Oracle SCOM Agent Agent account as a user role member.
6. Click **Next** to go to the Approve targets page.
7. Select the targets that you want the Oracle SCOM Agent to access.

   These are the target types for the alerts that the Oracle SCOM Agent will handle. Typically, you would use the default “All targets are automatically approved, including targets in Management Packs imported in the future.”
8. Click **Next** to go to the Approve groups page.
9. Select the groups that you want the Oracle SCOM Agent to access. You would generally want to use the default of all groups.
10. Click **Next** to go to the Approve tasks page.
11. Click **Next** to go to the Approve views page.
12. Click **Next** to go to the Summary page.

13. Click **Create** to create the Oracle SCOM Agent user role.

2.2.3 Installing the Agent

The SCOM Web Service uses the back-end Oracle SCOM Agent to access the SCOM API. The Oracle SCOM Agent must be installed on a Windows system that has connectivity to the SCOM Root Management Server (RMS). The Oracle SCOM Agent is preconfigured to interface with the SCOM Web Service and requires minimal configuration.

Note: There should only be one installed instance of the Oracle SCOM Agent.

To install the Oracle SCOM Agent, perform the following steps:

1. Download the connector binaries from Oracle Technology Network and put the SCOMAgent.zip installation file into the directory where you want to install the Oracle SCOM Agent.
2. Unzip the contents of the SCOMAgent.zip file to any directory.

   This creates the SCOMAgentInstaller.msi and the OracleEnterpriseManager.Alert.Creator.xml files in the designated directory.
3. Navigate to the directory and run the Oracle SCOM Agent installer by double-clicking on the SCOMAgentInstaller.msi file.

   This starts the installer and displays the Welcome to the Oracle SCOM Agent Setup Wizard page.
4. Click **Next** to display the Service Type page.
5. Select the type of service to be installed under IIS. The default and recommended service type is Web Site.

   This installs the service as a stand-alone web site. Selecting Virtual Directory installs the service as a Virtual Directory under an existing web site.
6. Click **Next** to display the Select Installation Folder page.
7. Enter the location to install the Agent or accept the default location of C:\iWaveSoftware\SCOMConnectorAgent .
8. Click **Next** to display the Oracle SCOM Agent Options page.
9. Enter the name to use when registering the connector in SCOM, or accept the default value of Oracle SCOM Agent.
10. Click **Next** to display the Confirm Installation page.
11. Click **Next** to display the SCOM Management Group Configuration page, and enter the information for the following required fields on the form:
    - Host name or IP address of the RMS server
    - Domain of the account to use when connecting to the SCOM API
    - User name of the account to use when connecting to the SCOM API
    - Password of the account to use when connecting to the SCOM API

Note: The information for the account from Section 2.2.2, "Setting Up the Agent Account" should be entered in the Domain, Username, and Password fields.

12. Click **Done** to proceed. The window displayed next depends on the Service Type you selected in step 5 above.
    - If you selected Web Site:

      The Web Site Configuration window appears. This window contains the Web Site Name and Port Number fields, and both have default values. Accept the default values or change them to the desired values.
    - If you selected Virtual Directory:

      The Virtual Directory Configuration window appears. This window defines the name of the virtual directory to create and the web site within which it will be installed. Accept the default values or change them to the desired values.
13. For either window, click **OK** to proceed and display the Web Service Credentials window. This window defines the credentials to specify when testing the newly installed Oracle SCOM Agent.
14. Specify valid Windows account credentials and click **OK**.

    The installer now invokes the web service to verify that it is operational. A window pops up with the results of the test.
15. Close the window. The Installation Successful window appears. This window lists the URL of the Oracle SCOM Agent.

    Note the URL. You will need this whenever you install the SCOM Web Service.
16. Click **OK** to continue. The Installation Complete window appears.
17. Click **Close** to complete the Agent installation process.

2.2.4 Installing the Alert Creator Management Pack

A management pack file named OracleEnterpriseManager.Alert.Creator.xml is also included in the Agent installation zip file. This management pack is required to create alerts in SCOM. If you are going to forward Enterprise Manager alerts to SCOM, follow the steps below to import the management pack into SCOM.

1. In the Administration pane of the OpsMgr console, select **Administration**, then **Management Packs**.
2. Right-click on **Management Packs** and select **Import Management Pack…** The Select Management Packs to Import window appears.
3. Navigate to the directory where the OracleEnterpriseManager.Alert.Creator.xml file is located.
4. Select the **OracleEnterpriseManager.Alert.Creator.xml** file and click **Open**. The Import Management Packs window appears.

Note: Depending on the version of SCOM that you are running, you might see the following error when you attempt to open the management pack:

```
OracleEnterpriseManager Alert Creator
The OracleEnterpriseManager Alert Creator Management Pack will fail
to import because it depends on the following Management Packs:
System.Library version 6.0.6278.0
Microsoft.SystemCenter.Library version 6.0.6278.0
System.Health.Library version 6.0.6278.0
Microsoft.Windows.Library version 6.0.6278.0
Please add them to the list by clicking on the Add... button and
searching in your machine.
```

If you see this error, you need to use a text editor to change four management packs referenced in the References section of the management pack file. The version number information must be updated to match the version numbers used in your system

5. Click **Import** to import the management pack.
6. Click **Close** after the management pack has been imported.

The Agent is now configured to insert alerts into SCOM.

2.2.5 Starting and Stopping the Agent

The installer automactically starts the Agent. To stop the agent, open the IIS manager, select the web site where it was installed, then click **Stop**. To start, click **Start**.

2.3 Installing the Microsoft SCOM Web Service

The SCOM web service acts as a front-end for all data flowing into and out of SCOM. Oracle Enterprise Manager posts calls to the web service whenever it needs to create or update an alert, or get new or updated alerts from SCOM.

You can install the SCOM web service on any Unix or Windows system that has connectivity to the Oracle SCOM Agent and the Oracle Enterprise Manager server.

2.3.1 Installing and Running the Microsoft SCOM Web Service on Unix

The following sections explain how to install and then subsequently run the Web Service.

2.3.1.1 Installing the Web Service on Unix

To install the web service on a Unix platform, perform the following steps:

1. Create a directory where you want to install the web service.
2. Open a terminal and change the working directory to the installation directory.
3. Download the SCOM_webservices_adapter.jar file from the Oracle Technology Network to the installation directory, then extract the component .jar files.
4. Make sure the JAVA_HOME environment variable is set to the directory where Java 1.6 is installed.
5. Enter the following command to unzip and extract the .jar file:

```
$JAVA_HOME/bin/jar xvf SCOM_webservices_adapter.jar
```

This creates the adapters directory that contains the installation files.

Note: If the system where the SCOM web service is being installed does not have the JDK installed, you cannot extract the jar file contents. You need to copy the jar file to a system that has the JDK installed and transfer the files after they have been extracted.

6. Enter the following command to change the working directory:

   ```
   cd adapters/endpoints/SCOM2007
   ```

7. Enter the following command to run the installation script:

   ```
   sh ./install.sh
   ```

8. When the script prompts whether you want to use HTTPS:
   - If you specify Y, the web service is set up to use HTTPS port number 8443.
   - If you specify N, the web service is set up to use HTTP port number 8080.
9. When the script prompts for the user name of the web service, enter the user name that must be provided to access the SCOM Web Service.
10. When the script prompts for the password of the web service, enter the password that must be provided to access the SCOM Web Service.
11. After the script prompts for the URL of the Oracle SCOM Agent, enter the URL that was noted when you installed the Oracle SCOM Agent.
12. After the script prompts for the username and password to use when accessing the Agent, enter a valid windows username and password.
13. After the the script displays the message "SCOM Web Service Complete," press Enter to complete the installation.
14. If the web service was configured to run using the HTTPS protocol, you must install a SSL certificate. You can install a self-signed certificate, or you can acquire a certificate from a Certificate Authority (CA).
    - To generate and install a self-signed SSL certificate, enter the following commands, and replace <hostname> with the system host name or IP address that the SCOM web service will use:

      ```
      "%JAVA_HOME%\bin\keytool" -delete -alias iwave -keypass iwavepw -storepass
      iwavepw -keystore keystore.jks

      "%JAVA_HOME%\bin\keytool" -genkey -alias iwave -keyalg RSA -keysize 1024
      -dname "CN=<hostname>, OU=Development, O=iWave Software, L=Frisco, ST=TX,
      C=US" -keypass iwavepw -storepass iwavepw -keystore keystore.jks
      ```

    - To install a certificate that the Certificate Authority issues:
      – Request a certificate from a Certificate Authority, such as VeriSign.

        In the certificate request, make sure to specify the host name or IP address that the SCOM web service will use. The host name in the certificate must match the host name configured for the web service. If they do not match, the web service cannot function.

– After you obtain the certificate from the Certificate Authority, enter the following command to install the certificate, where <certificateFile> is the full path name of the file provided by the Certificate Authority:

```
"%JAVA_HOME%\bin\keytool" -export -alias iwave -file <certificateFile>
-keypass iwavepw -storepass iwavepw -keystore keystore.jks
```

The web service framework is now installed and ready to start.

If the Microsoft SCOM Web Service was configured to use the HTTPS protocol, the certificate must be imported into Enterprise Manager. See Section 2.3.3, "Adding Signed Certificates to Enterprise Manager" for instructions.

2.3.1.2 Running the Web Service on Unix

To run the Microsoft SCOM Web Service framework commands listed with the following tasks, first change the working directory to ...

adapters/bin

... in the installation directory.

- **Start** — ./service.sh start
- **Shut Down** — ./service.sh stop
- **Restart** — ./service.sh restart
- **Check Status** — ./service.sh status

2.3.1.3 Testing the Web Service on Unix

Perform the following steps to verify that the Microsoft SCOM Web Service is functional.

1. Open a terminal and change the working directory to the adapters/bin directory in the installation directory.
2. Enter the following command to run the test script:

   ```
   ./testAdapter.sh
   ```

3. When the utility prompts for the web service password, enter the password you specified for the SCOM web service in step 10 of section Section 2.3.1.1, "Installing the Web Service on Unix".
4. If the test completes successfully, the last line the utility displays is "Test completed successfully."

> **Note:** If the HTTPS protocol is being used, the test fails if the installed JRE version is 1.6_10. An issue with this version causes the test to fail. To test the web service, you need to verify that you can load the WSDL in a web browser. See "Testing the Microsoft SCOM Connector" on page 3-5.

2.3.2 Installing and Running the Microsoft SCOM Web Service on Windows

The following sections explain how to install and then subsequently run the Web Service.

2.3.2.1 Installing the Web Service on Windows

To install the web service on a Windows platform, perform the following steps:

1. Create a directory where you want to install the web service.
2. Open a terminal and change the working directory to the installation directory.
3. Download the SCOM_webservices_adapter.jar file from the Oracle Technology Network to the installation directory, then extract the component .jar files.
4. Make sure the JAVA_HOME environment variable is set to the directory where Java 1.6 is installed.
5. Enter the following command to unzip and extract the .jar file:

   ```
   %JAVA_HOME%\bin\jar xvf SCOM_webservices_adapter.jar
   ```

   This creates the adapters directory that contains the installation files.

   Note: If the system where the SCOM web service is being installed does not have the JDK installed, you cannot extract the jar file contents. You need to copy the jar file to a system that has the JDK installed and transfer the files after they have been extracted.

6. Enter the following command to change the working directory:

   ```
   cd adapters\endpoints\SCOM2007
   ```

7. Enter the following command to run the installation script:

   ```
   .\install.bat
   ```

8. When the script prompts whether you want to use HTTPS:
   - If you specify Y, the web service is set up to use HTTPS port number 8443.
   - If you specify N, the web service is set up to use HTTP port number 8080.
9. After the script prompts for the URL of the Oracle SCOM Agent, enter the URL that was noted when you installed the Oracle SCOM Agent.
10. After the script prompts for the username and password to use when accessing the Agent, enter a valid windows username and password.
11. After the script displays the message "SCOM Web Service Complete," click Enter to complete the installation.
12. If the web service was configured to run using the HTTPS protocol, you must install a SSL certificate. You can install a self-signed certificate, or you can acquire a certificate from a Certificate Authority (CA).
    - To generate and install a self-signed SSL certificate, enter the following commands, and replace <hostname> with the system host name or IP address that the SCOM web service will use:

      ```
      cd ..\..\conf

      "%JAVA_HOME%\bin\keytool" -delete -alias iwave -keypass iwavepw -storepass
      iwavepw -keystore keystore.jks

      "%JAVA_HOME%\bin\keytool" -genkey -alias iwave -keyalg RSA -keysize 1024
      -dname "CN=<hostname>, OU=Development, O=iWave Software, L=Frisco, ST=TX,
      C=US" -keypass iwavepw -storepass iwavepw -keystore keystore.jks
      ```

- To install a certificate that the Certificate Authority issues:
  - Request a certificate from a Certificate Authority, such as VeriSign.

    In the certificate request, make sure to specify the host name or IP address that the SCOM web service will use. The host name in the certificate must match the host name configured for the web service. If they do not match, the web service cannot function.
  - After you obtain the certificate from the Certificate Authority, enter the following command to install the certificate, where <certificateFile> is the full path name of the file provided by the Certificate Authority:

    ```
    cd ..\..\conf

    "%JAVA_HOME%\bin\keytool" -export -alias iwave -file <certificateFile>
    -keypass iwavepw -storepass iwavepw -keystore keystore.jks
    ```

The following steps are optional. If you want the web service to run as a Windows service, perform the following steps.

1. Change the working directory to the adapters\bin directory in the installation directory.
2. Enter the following command to install the web service as a Windows service:

   ```
   service.bat install
   ```

The web service framework is now installed and ready to start.

If the Microsoft SCOM Web Service was configured to use the HTTPS protocol, the certificate must be imported into Enterprise Manager. See Section 2.3.3, "Adding Signed Certificates to Enterprise Manager" for instructions.

2.3.2.2 Running the Web Service on Windows

Standalone Service

To start the SCOM web service framework when set up as a standalone application (not set up to run as a Windows service):

1. Change the working directory to the adapters\bin directory in the installation directory.
2. Run the following command:

   ```
   startAdapters.bat
   ```

To shut down the SCOM web service framework, close the window where you started the adapter.

Windows Service

To start the SCOM web service framework when set up to run as a Windows service, enter the following command:

```
net start iWaveAdapters
```

To shut down the SCOM web service framework, enter the following command:

```
net stop iWaveAdapters
```

2.3.2.3 Testing the Web Service on Windows

Perform the following steps to verify that the Microsoft SCOM Web Service is functional.

1. Open a terminal and change the working directory to the adapters\bin directory in the installation directory.
2. Enter the following command to run the test script:

   ```
   .\testAdapter.bat
   ```

3. When the utility prompts for the web service password, enter the password you specified for the SCOM web service in step 10 of section Section 2.3.2.1, "Installing the Web Service on Windows" (Windows).
4. If the test completes successfully, the last line the utility displays is "Test completed successfully."

> **Note:** If the HTTPS protocol is being used, the test fails if the installed JRE version is 1.6_10. An issue with this version causes the test to fail. To test the web service, you need to verify that you can load the WSDL in a web browser. See "Testing the Microsoft SCOM Connector" on page 3-5.

2.3.3 Adding Signed Certificates to Enterprise Manager

The Service Manager SSL certificate must be imported into Enterprise Manager. For versions 10.2.0.4 and 10.2.0.5, perform the steps in Adding Signed Certificates to Wallet Manager. For version 11.1.0.1, perform the steps in Adding Signed Certificates to cacerts.

2.3.3.1 Adding Signed Certificates to Wallet Manager

> **Note:** Oracle Wallet Manager is available at $ORACLE_HOME/bin on OMS for versions 10.2.0.4 and 10.2.0.5. See the *Oracle Application Server Administrator's Guide* for details.

Perform the following steps in Oracle Enterprise Manager to add signed certificates:

1. Do the following to obtain a copy of the certificate that the OVO web service is using:
   a. Open a command prompt window and change the working directory to ...

      ```
      <SCOMWS_INSTALL>/adapters/conf
      ```

      ... where <SCOMWS_INSTALL> is the directory where the OVO web service is installed.

   b. Issue the following command to extract the certificate:

      — Unix platforms:

      ```
      $JAVA_HOME/bin/keytool -exportcert -alias iwave -file SCOMws.cer -keystore
      keystore.jks -storepass iwavepw
      ```

      — Windows platforms:

      ```
      "%JAVA_HOME%\bin\keytool" -exportcert -alias iwave -file SCOMws.cer
      ```

```
-keystore keystore.jks -storepass iwavepw
```

c. Transfer the certificate file SCOMws.cer to the system where Enterprise Manager is installed.

2. Open a new terminal and set the `ORACLE_HOME` environment variable to the directory where OMS is installed.
3. As Super Administrator, create a wallet using the following `orapki utility` command at the OMS host:

```
orapki wallet create -wallet client -auto_login
```

4. Add the trusted certificate to the wallet by entering the following command:

```
orapki wallet add -wallet client -trusted_cert -cert <certFile>
```

5. To view the content of the wallet, enter the following command:

```
orapki wallet display -wallet client
```

Verify that the certificate that was added is listed in the Trusted Certificates.

6. Start Oracle Wallet Manager and open the client wallet.
7. Click on Trusted Certificates and select **Operations** on the main menu.
8. Select **Export All Trusted Certificates**.
9. Save the file as `certdb.txt`.
10. Place the file `certdb.txt` in the connector home root directory (`$OMS_HOME/sysman/connector`).

    If the `certdb.txt` file already exists in the root directory, open the file and add the contents of your `certdb.txt` file to the existing content.

Java SSL can now use this file for communication between Oracle Enterprise Manager and the SCOM web service in HTTPS mode.

> **See Also:** For additional information on creating a wallet, see "Creating and Viewing Oracle Wallets with orapki" in the *Oracle Database Advanced Security Administrator's Guide, 10g Release 2 (10.2).*

2.3.3.2 Adding Signed Certificates to cacerts

Do the following in Enterprise Manager to add signed certificates to the Java cacerts keystore:

1. Copy the certificate to the Enterprise Manager server system.
2. Determine the location of the JRE in the Oracle Home directory.
3. Open a command window and navigate to the JRE bin directory.
4. Enter the following command to add the certificate to the cacerts keystore:

```
keytool -importcert -keystore ..\lib\security\cacerts -storepass changeit
-trustcacerts -file <certfile> -alias scomws_cert
```

5. Restart OMS by opening a command window, changing the working directory to `<ORACLE_HOME>/oms10g/bin`, and issuing the following commands:

```
emctl stop oms
emctl start oms
```

2.3.4 Oracle Enterprise Manager Alert Polling to SCOM

After installation and configuration, the alert connector automatically polls the SCOM web service for alerts to exchange alerts with Oracle Enterprise Manager. The poll cycle is configurable; the duration is specified in minutes with a minimum possible duration of 5 minutes.

For every poll cycle, the alert connector polls for up to (40 * polling interval) new or updated alerts in SCOM. The Oracle Enterprise Manager connector framework processes and acknowledges all of the alerts provided in the poll response.

2.4 Installing the Microsoft SCOM Connector in Oracle Enterprise Manager

The following procedure explains how to add the new SCOM Connector.

Note: Table 2–1 provides descriptions for the parameters shown for the emctl command in this procedure.

---

1. Copy `scom_connector.jar` to `$ORACLE_HOME/sysman/connector` on the server hosting your OMS. For multiple OMSes, you need to copy the `.jar` file for all OMSes.
2. Run the following emctl command on all OMSes if you have a multi-OMS environment:

```
$OMS_HOME/bin/emctl extract_jar connector -jar <jarfile> -cname
<connector_name>
```

Note: The commands in this section and the following section reference the `OMS_HOME` environment variable. `OMS_HOME` must be set to the OMS sub-directory in the Enterprise Manager installation directory. For versions 10.2.0.4 and 10.2.0.5, this is the oms10g directory. For version 11.1.0.1, this is the oms11g directory. Example settings of the OMS_HOME variable are `/gc/OracleHomes/oms10g` on a Unix platform running version 10.2.0.5, and `C:\Oracle\Middleware2\oms11g` on a Windows platform running version 11.1.0.1.

This extracts the scom_connector.jar file to the following folder:

```
$OMS_HOME/sysman/connector/SCOM_Connector/
```

For example:

```
emctl extract_jar connector -jar scom_connector.jar -cname "SCOM Connector"
```

3. Deploy the connector by running the following emctl command based on the Enterprise Manager version. You only need to run this step on one OMS.

11.1.0.1

```
$OMS_HOME/bin/emctl register_connector connector -dd
 <connectorType.xml> repos_pwd <password>
```

10.2.0.5

```
$OMS_HOME/bin/emctl register_connector connector -dd
 <connectorType.xml> -cs //<server>:<port>/<databaseSID>
 -repos_user <username> -repos_pwd <password>
```

For example:

```
$OMS_HOME/bin/emctl register_connector connector -dd $OMS_HOME/
sysman/connector/SCOM_Connector/SCOMConnector.xml -repos_pwd $repospwd
```

The new SCOM connector should now appear in the Management Connectors page after the emctl register_connector command has loaded the connector, as shown in Figure 2–2.

Figure 2–2 Installed SCOM Connector

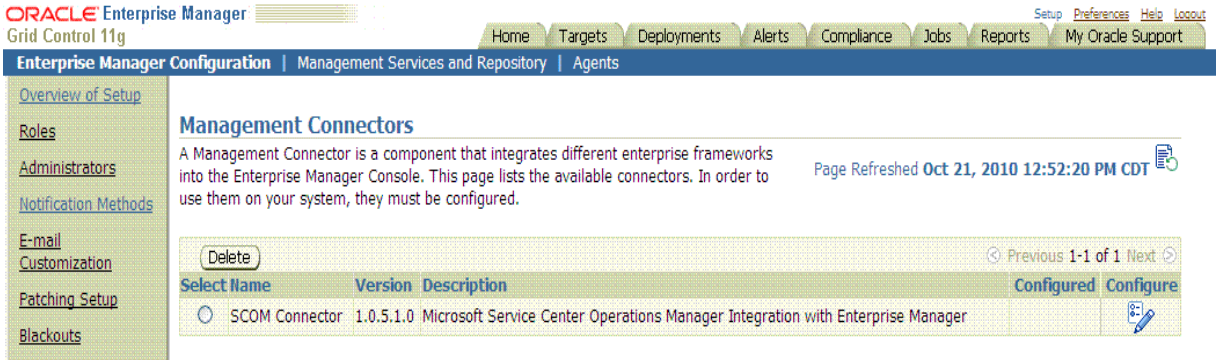


Table 2–1 provides descriptions for the parameters shown in the procedure above.

Table 2–1 emctl Parameters

Parameter	Description
`cname`	Connector name. Specify `"SCOM Connector"`. The double quotes ("") are mandatory.
`connectorType.xml`	Fully-qualified name of the connector deployment file. This SCOMConnector.xml file resides in the SCOM connector directory: $OMS_HOME/sysman/connector/SCOM_Connector/
`cs`	Connect string. Specify as "//$emHost:$dbPort/$dbSID", where, $emHost is the server, $dbPort is the port, and $dbSID is the database session identifier.
`ctname`	Connector type name. Specify `"SCOM Connector"`. The double quotes ("") are mandatory.
`database sid/ Service Name for RAC DB`	Repository database instance ID or service name if you are using a RAC database as the repository.
`description`	Short description for the ticket template. This description is also displayed in Enterprise Manager.
`iname`	Internal name — Depending on the template, the values can be acknowledgeAlerts, createEvent, getNewAlerts, getUpdatedAlerts, or updateEvent.
`jarfile`	Name of the jar file that contains the connector files. The file name is scom_connector.jar for the SCOM connector.
`port`	Listener port of the repository.

Table 2–1 (Cont.) emctl Parameters

Parameter	Description
repos_pwd	Password for SYSMAN.
repos_user	Specify SYSMAN.
server	Host name of the Enterprise Manager repository.
tname	Template name — Depending on the template, the values can be Acknowledge Alerts, Create Event, Get New Alerts, Get Updated Alerts, or Update Event.
ttype	Template type — Specify 1 for inbound transformation and 2 for outbound transformation.

2.5 Registering Templates

Before proceeding, if you are using SCOM version R2 in the integration, no changes are required to the template files. If you are using a version prior to R2 of SCOM, make the following changes to the templates before registering:

1. Open the createEvent_request.xsl file in a text editor.
2. Change the contents of the preSCOMR2 variable on line 6 from false to true.
3. Save the changes and close the file.

After you have done this, run the following emctl register_template connector command for each template. The command must specify a user with execute privilege on emctl and the ability to read the template:

11.1.0.1

```
$OMS_HOME/bin/emctl register_template connector -t <template.xml> -repos_pwd
<password> -ctname <connector_type_name> -cname <connector_name> -iname <internal_
name> -tname <template_name> -ttype <template_type> -d <description>
```

10.2.0.5

```
$OMS_HOME/bin/emctl register_template connector -t <template.xml> -cs
//<server>:<port>/<dbSID> -repos_user <username> -repos_pwd <password> -ctname
<connector_type_name> -cname <connector_name> -iname <internal_name> -tname
<template_name> -ttype <template_type> -d <description>
```

Replace <template.xml>, <internal_name>, <template_name> and <template_type> with the values listed in Table 2–2.

Table 2–2 Possible Replacement Values for register_template Parameters

template.xsl and template.xml	internal_name	template_name	template_type
acknowledge_request.xsl	acknowledgeAlerts	Acknowledge Alerts	2
cleanup_request.xml	cleanup	Cleanup	3
cleanup_request.xsl	cleanup	Cleanup	2
createEvent_request.xsl	createEvent	Create Event	2
createEvent_response.xsl	createEvent	Create Event	1
generic_request_ acknowledgealerts.xml	acknowledgeAlerts	Acknowledge Alerts	3

Table 2–2 (Cont.) Possible Replacement Values for register_template Parameters

template.xsl and template.xml	internal_name	template_name	template_type
getNewAlerts_request.xsl	getNewAlerts	Get New Alerts	2
getNewAlerts_response.xsl	getNewAlerts	Get New Alerts	1
getUpdatedAlerts_request.xsl	getUpdatedAlerts	Get Updated Alerts	2
getUpdatedAlerts_ response.xsl	getUpdatedAlerts	Get Updated Alerts	1
setup_request.xml	setup	Setup	3
setup_request.xsl	setup	Setup	2
setup_response.xsl	setup	Setup	1
updateEvent_request.xsl	updateEvent	Update Event	2
updateEvent_response.xsl	updateEvent	Update Event	1
template_type Key:			
template_type1 — Inbound transformation template_type 2 — Outbound transformation template_type 3 — XML outbound transformation			

The following examples are based on the template values shown in Table 2–2.

Example 2–1 Request XSL File for acknowledgeAlerts Method

```
$OMS_HOME/bin/emctl register_template connector -t $OMS_HOME/sysman/connector/
SCOM_Connector/acknowledge_request.xsl -repos_pwd <password> -ctname "SCOM
Connector" -cname "SCOM Connector" -tname "Acknowledge Alerts" -iname
"acknowledgeAlerts" -ttype 2 -d "This is the request xsl file for
acknowledgeAlerts method"
```

Example 2–2 Request XML File for Cleanup Method

```
$OMS_HOME/bin/emctl register_template connector -t $OMS_HOME/sysman/connector/
SCOM_Connector/cleanup_request.xml -repos_pwd <password> -ctname "SCOM Connector"
-cname " SCOM Connector " -tname "Cleanup Request" -iname "cleanup" -ttype 3 -d
"This is the request xml file for cleanup method"
```

Example 2–3 Request XSL File for Cleanup Method

```
$OMS_HOME/bin/emctl register_template connector -t $OMS_HOME/sysman/connector/
SCOM_Connector/cleanup_request.xsl -repos_pwd <password> -ctname "SCOM Connector"
-cname "SCOM Connector" -tname "Cleanup Request" -iname "cleanup" -ttype 2 -d
"This is the request xsl file for cleanup method"
```

Example 2–4 Request XSL File for createEvent Method

```
$OMS_HOME/bin/emctl register_template connector -t $OMS_HOME/sysman/connector/
SCOM_Connector/createEvent_request.xsl -repos_pwd <password> -ctname "SCOM
Connector" -cname "SCOM Connector" -tname "Create Event Request" -iname
"createEvent" -ttype 2 -d "This is the request xsl file for createEvent method"
```

Example 2–5 Response XSL File for createEvent Method

```
$OMS_HOME/bin/emctl register_template connector -t $OMS_HOME/sysman/connector/
SCOM_Connector/createEvent_response.xsl -repos_pwd <password> -ctname "SCOM
```

```
Connector" -cname "SCOM Connector" -tname "CreateEvent Response" -iname
"createEvent" -ttype 1 -d "This is the response xsl file for createEvent method"
```

Example 2–6 Request XML File for acknowledgeAlerts Method

```
$OMS_HOME/bin/emctl register_template connector -t $OMS_HOME/sysman/connector/
SCOM_Connector/generic_request_acknowledgealerts.xml -repos_user SYSMAN -repos_pwd
<password> -ctname "SCOM Connector" -cname "SCOM Connector" -tname "Acknowledge
Alerts" -iname "acknowledgeAlerts" -ttype 3 -d "This is the request xml file for
acknowledgeAlerts method"
```

Example 2–7 Request XSL File for getNewAlerts Method

```
$OMS_HOME/bin/emctl register_template connector -t $OMS_HOME/sysman/connector/
SCOM_Connector/getNewAlert_request.xsl -repos_pwd <password> -ctname "SCOM
Connector" -cname "SCOM Connector" -tname "Get New Alerts Request" -iname
"getNewAlerts" -ttype 2 -d "This is the request xsl file for getNewAlerts method"
```

Example 2–8 Response XSL File for getNewAlerts Method

```
$OMS_HOME/bin/emctl register_template connector -t $OMS_HOME/sysman/connector/
SCOM_Connector/getNewAlerts_response.xsl -repos_pwd <password> -ctname "SCOM
Connector" -cname "SCOM Connector" -tname "Get New Alerts Response" -iname
"getNewAlerts" -ttype 1 -d "This is the response xsl file for getNewAlerts method"
```

Example 2–9 Request XSL File for getUpdatedAlerts Method

```
$OMS_HOME/bin/emctl register_template connector -t $OMS_HOME/sysman/connector/
SCOM_Connector/getUpdatedAlert_request.xsl -repos_pwd <password> -ctname "SCOM
Connector" -cname "SCOM Connector" -tname "Get Updated Alerts Request" -iname
"getUpdatedAlerts" -ttype 2 -d "This is the request xsl file for getUpdatedAlerts
method"
```

Example 2–10 Response XSL File for getUpdatedAlerts Method

```
$OMS_HOME/bin/emctl register_template connector -t $OMS_
HOME/sysman/connector/SCOM_Connector/getUpdatedAlerts_response.xsl -repos_pwd
<password> -ctname "SCOM Connector" -cname "SCOM Connector" -tname "Get Updated
Alerts Response" -iname "getUpdatedAlerts" -ttype 1 -d "This is the response xsl
file for getUpdatedAlerts method"
```

Example 2–11 Request XML File for Setup Method

```
$OMS_HOME/bin/emctl register_template connector -t $OMS_HOME/sysman/connector/
SCOM_Connector/setup_request.xml -repos_pwd <password> -ctname "SCOM Connector"
-cname "SCOM Connector" -tname "Setup Request" -iname "setup" -ttype 3 -d "This is
the request xml file for setup method"
```

Example 2–12 Request XSL File for Setup Method

```
$OMS_HOME/bin/emctl register_template connector -t $OMS_
HOME/sysman/connector/SCOM_Connector/setup_request.xsl -repos_pwd <password>
-ctname "SCOM Connector" -cname "SCOM Connector" -tname "Setup Request" -iname
"setup" -ttype 2 -d This is the request xsl file for setup method"
```

Example 2–13 Response XSL File for Setup Method

```
$OMS_HOME/bin/emctl register_template connector -t $OMS_
HOME/sysman/connector/SCOM_Connector/setup_response.xsl -repos_pwd <password>
-ctname "SCOM Connector" -cname "SCOM Connector" -tname "Setup Response" -iname
"setup" -ttype 1 -d "This is the response xsl file for setup method"
```

Example 2–14 Request XSL File for updateEvent Method

```
$OMS_HOME/bin/emctl register_template connector -t $OMS_
HOME/sysman/connector/SCOM_Connector/updateEvent_request.xsl -repos_pwd <password>
-ctname "SCOM Connector" -cname "SCOM Connector" -tname "Update Event Request"
-iname "updateEvent" -ttype 2 -d "This is the request xsl file for updateEvent
method"
```

Example 2–15 Response XSL File for updateEvent Method

```
$OMS_HOME/bin/emctl register_template connector -t $OMS_
HOME/sysman/connector/SCOM_Connector/updateEvent_response.xsl -repos_pwd
<password> -ctname "SCOM Connector" -cname "SCOM Connector" -tname "UpdateEvent
Response" -iname "updateEvent" -ttype 1 -d "This is the response xsl file for
updateEvent method"
```

3

Configuring the Connector

This chapter provides procedures to configure the two sub-pages of the main Configure Management Connector page, then explains how to perform other tasks to complete the configuration process.

This chapter discusses the following topics:

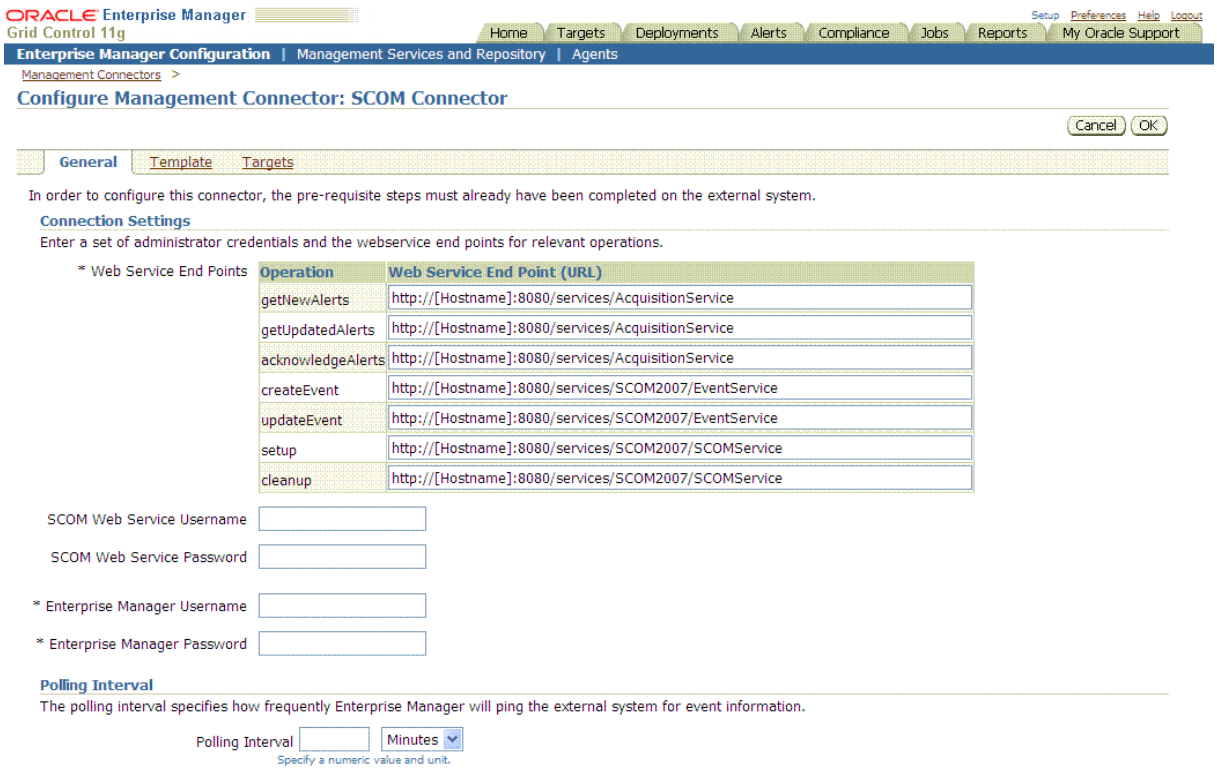
- Configuring the General Page
- Configuring the Targets Page
- Adding a Subscription in SCOM
- Testing the Microsoft SCOM Connector
- Sending Oracle Enterprise Manager Alerts to Microsoft SCOM
- Sending Microsoft SCOM Alerts to Oracle Enterprise Manager
- Generating Test Alerts in Microsoft SCOM

3.1 Configuring the General Page

To configure the General page:

1. From the Management Connectors page, select the **SCOM Connector** and click the **Configure** icon. By default, the General sub-page of the Configure Management Connector page appears, as shown in Figure 3–1.

Figure 3–1 SCOM Connector General Settings



2. Update the URLs for each of the Web Service End Point operations as described below.

   Operation Descriptions

   The SCOM connector uses the following operations (web methods) to exchange data with the SCOM Web Service.

   - **getNewAlerts** — Creates alerts in Oracle Enterprise Manager based on alerts that originate in Microsoft SCOM. Oracle Enterprise Manager uses this operation when polling for alerts in Microsoft SCOM.
   - **getUpdatedAlerts** — Updates alerts in Oracle Enterprise Manager based on alerts that originate from Microsoft SCOM. Oracle Enterprise Manager uses this operation when polling for alerts from Microsoft SCOM.
   - **acknowledgeAlerts** — Acknowledges the alerts after Oracle Enterprise Manager has processed them. Oracle Enterprise Manager uses this operation when polling for alerts in Microsoft SCOM.
   - **createAlert** — Generates alerts in Microsoft SCOM based on alerts that originate in Oracle Enterprise Manager. Oracle Enterprise Manager invokes this operation when it forwards a new alert to SCOM.
   - **updateAlert** — Updates alerts in Microsoft SCOM based on alerts that originate in Oracle Enterprise Manager. Oracle Enterprise Manager invokes this operation when it forwards an updated alert to SCOM.
   - **setup** — Registers the SCOM Agent with the SCOM RMS. This causes the SCOM Agent to appear as a product connector at the SCOM console. Oracle Enterprise Manager invokes this operation when the connector is configured.

- **cleanup** — Deregisters the SCOM Agent from the SCOM server. This causes the SCOM Agent to no longer appear as a product connector at the SCOM console. Oracle Enterprise Manager invokes this operation when the connector is deleted.

URL Types

The connector uses three different URLs for operations. One URL polls data out of Microsoft SCOM (`getNewAlerts`, `getUpdatedAlerts` and `acknowledgeAlerts`), and defaults to the following value:

```
http://[Hostname]:8080/services/AcquisitionService
```

Another URL pushes data into Microsoft SCOM (`createAlert` and `updateAlert`), and defaults to the following value:

```
http://[Hostname]:8080/services/SCOM2007/EventService
```

This URL is used for registration of the SCOM Agent with Microsoft SCOM (setup and cleanup), and defaults to the following value:

```
http://[Hostname]:8080/services/SCOM2007/SCOMService
```

You need to make the following changes to each of the default URLs:

- Replace `[Hostname]` in the URL with the hostname or IP address of the system where the SCOM Web Service is installed.
- If necessary, change the port to the port on which the web services are running. For example, the default port for HTTP is 8080 and the default port for HTTPS is 8443.
- If the SCOM Web Service was configured to use the HTTPS protocol, change http to https at the beginning of each web service URL.

If you are using HTTPS as the protocol, you must also include the SCOM web service certificate in Oracle Wallet Manager as described in Section 2.3.3, "Adding Signed Certificates to Enterprise Manager".

3. Enter the user name and password you specified when you installed the SCOM web service, which is discussed in steps 9 and 10 of Section 2.3.1.1, "Installing the Web Service on Unix", and steps 9 and 10 of Section 2.3.2.1, "Installing the Web Service on Windows".
4. Enter the user name and password of the Oracle Enterprise Manager account.
5. Optionally enter a polling interval to specify how often Oracle Enterprise Manager should poll the Microsoft SCOM web service for new or updated alerts to process. The poll interval defaults to 5 minutes if not specified.
6. Click **OK** to save your configuration changes.

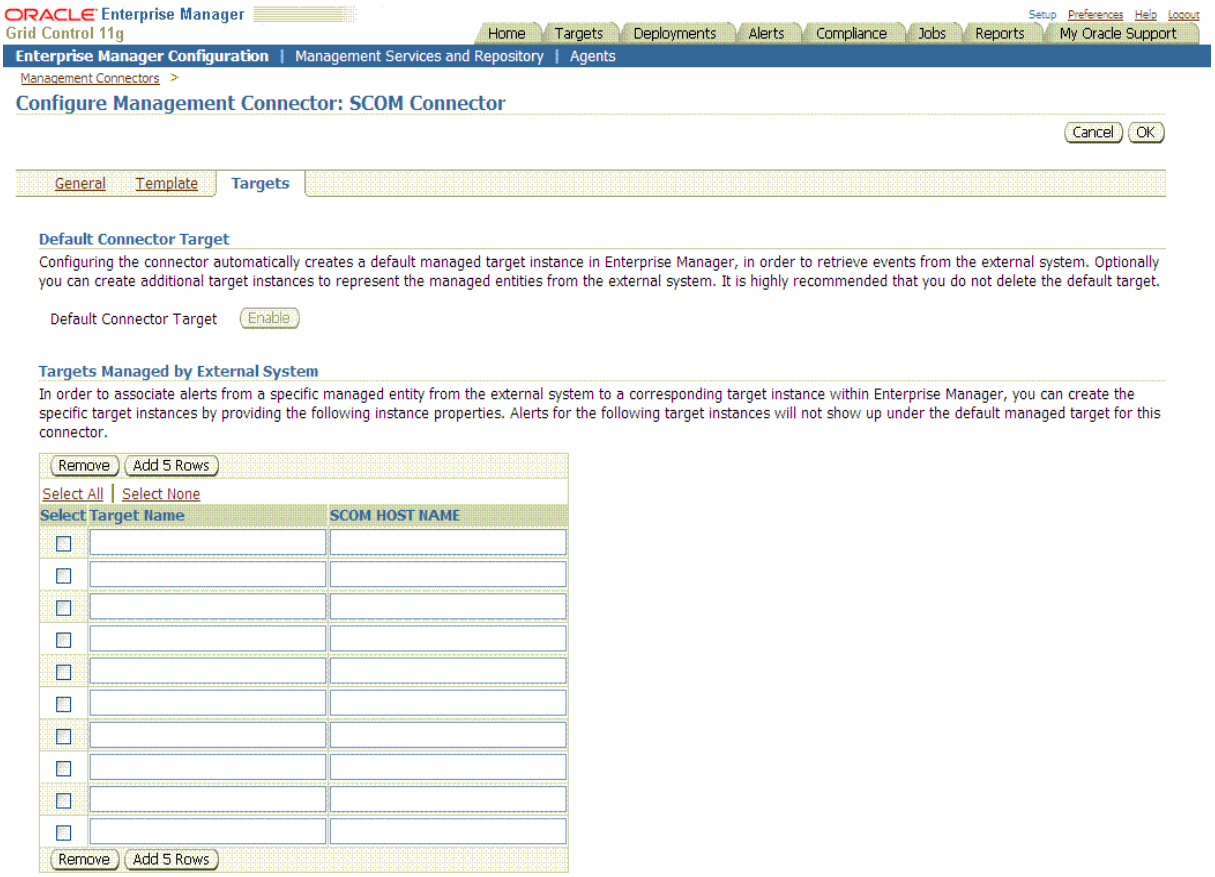
3.2 Configuring the Targets Page

Whenever a Microsoft SCOM alert is translated into an Oracle Enterprise Manager alert, the Microsoft SCOM alert host name determines the target-type instance associated with the alert in Oracle Enterprise Manager. If a target instance that matches the alert host name is not found, the default target instance of `generic_scom_managed_host` is used for the alert.

To add proxy targets in Oracle Enterprise Manager:

1. From the Configure Management Connector page, click the **Targets** link to display the Targets page, as shown in Figure 3–2.

Figure 3–2 SCOM Connector Target Settings



2. Provide a target name. The Target Name field is set to the host name specified in the SCOM alert and must exactly match the name.
3. Provide the SCOM host name in the SCOM HOST NAME field. This field must be set to the same value as the Target Name field.
4. Repeat this process for as many target instances as desired.
5. Click **OK** to save your configuration changes.

3.3 Adding a Subscription in SCOM

If you want to forward SCOM alerts to Enterprise Manager, you must add a subscription in SCOM to forward alerts to the SCOM Agent.

Perform the following steps to add a subscription in SCOM.

1. In the Administration pane of the SCOM console, select **Administration**, then **Notification**, then **Product Connectors**. The SCOM Agent should be listed as a product connector.
2. Right-click on the SCOM Agent and select **Properties** from the list of options to display the SCOM Agent – Product Connector Properties window.

3. Click **Add** in the Subscriptions section to display the Product Connector Subscription Wizard window.
4. Enter a subscription name and an optional description, then click **Next**.
5. Select the groups that you want alerts to be forwarded from, then click **Next**.
6. Select the targets for which you want alerts, then click **Next**.
7. Specify the alert filtering criteria, then click **Create**.

SCOM should now be ready to forward alerts to the SCOM Agent.

3.4 Testing the Microsoft SCOM Connector

Perform the following steps to test the connector:

1. Log in to the Oracle Enterprise Manager console by entering a user name with a 'Super Administrator' role, entering the appropriate password, then clicking **Login**.
2. Click the **Setup** link at the top right part of the window. The Overview of Setup page appears.
3. Click the **Management Connectors** link on the left side of the window. The Management Connectors page appears, which shows the installed connectors.
4. Click on the **Configure** icon associated with the SCOM Connector.
5. Click on the **General** tab.
6. Select and copy the URL specified for the `createAlert` or `updateAlert` operation.
7. Open an internet browser on the system where the Oracle Enterprise Manager server is installed.
8. In the address window, enter the URL that was copied in step 6 above. Add `?wsdl` to the end of the URL. The URL should appear similar to the following example:

   ```
   http://[Hostname]:8080/services/SCOM2007/EventService?wsdl
   ```

   `[Hostname]` is the actual host name or IP address where the SCOM web service is installed.

   If the WSDL is loaded, this confirms that the connector is configured correctly for sending alert information to SCOM.
9. At the Oracle Enterprise Manager console, select and copy the URL specified for the `getNewAlerts`, `getUpdatedAlerts`, or the `acknowledgeAlerts` operation. They should all be set to the same URL.
10. Open an internet browser on the system where the Oracle Enterprise Manager server is installed.
11. In the address window, enter the URL that you copied in step 9 above. Add `?wsdl` to the end of the URL. The URL should be similar to the following example:

    ```
    http://[Hostname]:8080/services/AcquisitionService?wsdl
    ```

    `[Hostname]` is the actual host name or IP address where the SCOM web service is installed.

    If the WSDL is loaded, this confirms that the connector is configured correctly for polling alert information from SCOM.

12. Select and copy the URL specified for the setup or cleanup operation.
13. Open an internet browser on the system where the Oracle Enterprise Manager server is installed.
14. In the address window, enter the URL that was copied in step 12 above. Add `?wsdl` to the end of the URL. The URL should appear similar to the following example:

    ```
    http://[Hostname]:8080/services/SCOM2007/SCOMService?wsdl
    ```

    `[Hostname]` is the actual host name or IP address where the SCOM web service is installed.

    If the WSDL is loaded, this confirms that the connector is configured correctly for registering in SCOM.

3.5 Sending Oracle Enterprise Manager Alerts to Microsoft SCOM

Alerts generated or updated in Oracle Enterprise Manager are not transferred to SCOM unless you create notification rules to invoke the Microsoft SCOM notification method. A notification rule identifies the conditions that must be met before the notification method is invoked.

The following sections provide procedures that explain how to create and update notification rules.

3.5.1 Creating Notification Rules

The following procedure explains how to create a new notification rule to invoke the SCOM notification method.

1. Click the **Preferences** link in the upper right corner of the Oracle Enterprise Manager console. The General page appears.
2. Click the **Notification Rules** link on the left side of the window. The Notification Rules page appears and displays a list of all defined notification rules.
3. Click **Create** to create a new notification rule.
4. From the **General** sub-page, enter a name for the notification rule and an optional description.

   Select the target type and whether you want it to apply to all targets of that type or a specific instance. If you indicate that you want a specific instance, you need to click **Add** and select the desired target instance.
5. Click the **Availability** link, then select the availability states for which you would like to receive notifications. Each state you select invokes the notification method whenever it is reached.
6. Click the **Metrics** link. If you want to trigger the notification method based on metric violations, click **Add** and select the metrics and states for which you want to invoke the notification method, then click **Continue**.
7. Click the **Actions** link. In the Advanced Notification Methods section, click the check box next to the SCOM Connector to assign the SCOM notification method to the notification rule.
8. Click **OK** to complete the setup.

3.5.2 Updating Notification Rules

The following procedure explains how to update an existing notification rule to invoke the SCOM notification method.

1. Click the **Preferences** link in the upper right corner of the Oracle Enterprise Manager console. The General page appears.
2. Click the **Notification Rules** link on the left side of the window. The Notification Rules page appears and displays a list of all defined notification rules.
3. Click on the radio button next to the notification rule you want to update, and click **Edit** to update the notification rule.
4. Click the **Actions** link. In the Advanced Notification Methods section, click on the check box next to the SCOM Connector to assign the SCOM notification method to the notification rule.
5. Click **OK** to complete the update.

3.5.3 Viewing Oracle Enterprise Manager Alerts

Whenever an alert is created in Microsoft SCOM from an alert that originates in Oracle Enterprise Manager, a link is provided in the alert text. To view the Oracle Enterprise Manager alert that triggered the alert, copy the URL to a web browser. You will be asked to log in to Oracle Enterprise Manager. After logging in, the Oracle Enterprise Manager alert information is displayed.

3.6 Sending Microsoft SCOM Alerts to Oracle Enterprise Manager

No special setup is required in Oracle Enterprise Manager to retrieve alert information from SCOM. Oracle Enterprise Manager automatically starts polling the SCOM web service after the connector has been configured.

SCOM does not automatically send new and updated alerts to the SCOM web service. You must define a subscription in SCOM to forward alerts to the SCOM Web Service. See Adding a Subscription in SCOM on page 3-4 for steps to add a subscription.

3.7 Generating Test Alerts in Microsoft SCOM

This section provides information for configuring SCOM to generate test alerts. If you already have a method of generating test alerts in SCOM, you can skip this section.

You need to perform the following tasks to generate a test alert in SCOM:

- Add a rule to SCOM that generates an alert whenever VBScript creates an error in the application log.
- Create a VBScript to add an error to the application log.

Adding a Rule in SCOM that Generates a Test Alert

1. In the Authoring pane of the OpsMgr console, select **Authoring**, then **Management Pack Objects**, then **Rules**.
2. Right-click on **Rules** and select **Create a new rule…** to display the The Create Rule Wizard window.
3. In the "Select the type of rule to create" pane, select **Alert Generating Rules**, then **Event Based**, then **NT Event Log (Alert)**, then click **Next**.

4. Enter the Rule Name (this can be anything), select a rule target of **Windows Server**, then click **Next**.
5. Make sure the Log name is set to Application, then click **Next**.
6. Right-click on the **And group** and select **Delete**.
7. Click **Insert**.
8. Click the **…** button in the expression that was inserted. A pop-up window should now appear.
9. Click on the **Select from a list of common event properties** radio button, select **EventSource** from the list under the radio button, then click **OK**.
10. Click on the **Operator** field and select **Equals**.
11. Click on the **Value** field, enter **WSH**, then click **Next**.
12. Enter the information that the alert is to generate. The generated information must meet the criteria specified in the subscription for the SCOM Agent.
13. Click **Create** to create the rule.

Creating a VBScript File to Add an Error to the Application Log

1. At the RMS system, create or identify the directory where the script will be located.
2. Open a new document in a text editor.
3. Copy the following VBScript commands into the new document:

```
set objShell = CreateObject("WScript.Shell")
objShell.LogEvent 1, "Test alert generated by VBScript"
```

4. Save the file as `createTestAlert.vbs` in the directory from step 1 above.

Running the File

Now run the file to create a test alert. You should create a new test alert every time you run the script.

4

Changing Default Configurations

This chapter explains how to change default mappings and default port numbers. This chapter discusses the following topics:

- Customizing Mappings
- Changing Default Port Numbers

4.1 Customizing Mappings

Although the default mappings are sufficient for most implementations, you can change them as needed. The following sections discuss:

- XML Format of Microsoft SCOM Alerts
- XML Format of Oracle Enterprise Manager Alerts
- Changing a Mapping

It is assumed that you already have a good understanding of XSL.

For reference information on the default mappings, see Appendix A, "Default Mappings".

4.1.1 XML Format of Microsoft SCOM Alerts

Example 4–1 represents the format that the Microsoft SCOM web service expects for creating new alerts in Microsoft SCOM. Example 4–2 represents the format that the Microsoft SCOM web service expects for updating alerts in Microsoft SCOM.

Example 4–1 Sample Create Format for Microsoft SCOM Web Service

```
<iwaveaf:create xmlns:iwaveaf="http://iwavesoftware.com/services/
  adapter-framework">
  <event>
    <summary></summary>
    <description></description>
    <severity></severity>
    <priority></priority>
    <extended-fields>
      <string-field name="CustomField1"></string-field>
      ...
      <string-field name="CustomField10"></string-field>
    </extended-fields>
  </event>
</iwaveaf:create>
```

Example 4–2 Sample Update Format for Microsoft SCOM Web Service

```
<iwaveaf:update xmlns:iwaveaf="http://iwavesoftware.com/services/
adapter-framework">
  <event>
    <identifier></identifier>
    <status></status>
    <extended-fields>
      <string-field name="AlertHistory"></string-field>
      <string-field name="CustomField1"></string-field>
      …
      <string-field name="CustomField10"></string-field>
    </extended-fields>
  </event>
</iwaveaf:update>
```

4.1.1.1 Mappings Between XML Format and Alert Field Names

Table 4–1 identifies the mappings between the Microsoft SCOM alert field names and the XML format that the Microsoft SCOM web services uses when creating an alert in SCOM. Table 4–2 identifies the mappings between the Microsoft SCOM alert field names and the XML format that the Microsoft SCOM web services uses when updating an alert in SCOM.

The XML document presented to the Microsoft SCOM web service must have the corresponding fields set. Fields denoted with an asterisk (*) are optional. This must be handled in the appropriate translation file identified in Table A–1.

Table 4–1 Create Alert Attributes and XML Path Mappings

Microsoft SCOM Slot Names	XML Path	Attribute Name	Attribute Value
Name	/create/event/summary		
Description	/create/event/severity		
Priority	/create/event/priority		
* Custom Field 1	/create/event/extended-fields/ string-field	name	CustomField1
* Custom Field 2	/create/event/extended-fields/ string-field	name	CustomField2
* Custom Field 3	/create/event/extended-fields/ string-field	name	CustomField3
* Custom Field 4	/create/event/extended-fields/ string-field	name	CustomField4
* Custom Field 5	/create/event/extended-fields/ string-field	name	CustomField5
* Custom Field 6	/create/event/extended-fields/ string-field	name	CustomField6
* Custom Field 7	/create/event/extended-fields/ string-field	name	CustomField7
* Custom Field 8	/create/event/extended-fields/ string-field	name	CustomField8
* Custom Field 9	/create/event/extended-fields/ string-field	name	CustomField9
* Custom Field 10	/create/event/extended-fields/ string-field	name	CustomField10

Table 4–2 Update Alert Attributes and XML Path Mappings

Microsoft SCOM Slot Names	XML Path	Attribute Name	Attribute Value
Id	/create/event/identifier		
Resolution State	/create/event/status		
* Custom Field 1	/create/event/extended-fields/ string-field	name	CustomField1
* Custom Field 2	/create/event/extended-fields/ string-field	name	CustomField2
* Custom Field 3	/create/event/extended-fields/ string-field	name	CustomField3
* Custom Field 4	/create/event/extended-fields/ string-field	name	CustomField4
* Custom Field 5	/create/event/extended-fields/ string-field	name	CustomField5
* Custom Field 6	/create/event/extended-fields/ string-field	name	CustomField6
* Custom Field 7	/create/event/extended-fields/ string-field	name	CustomField7
* Custom Field 8	/create/event/extended-fields/ string-field	name	CustomField8
* Custom Field 9	/create/event/extended-fields/ string-field	name	CustomField9
* Custom Field 10	/create/event/extended-fields/ string-field	name	CustomField10
* Alert History	/create/event/extended-fields/ string-field	name	AlertHistory

4.1.1.2 Extended Fields

Extended fields pass information for slots that are not mapped. An extended field is defined as a `<string-field/>` element that is a child of the extended-fields node. The name of the slot is specified in the name attribute, and the value of the slot is specified in the value attribute.

4.1.2 XML Format of Oracle Enterprise Manager Alerts

Example 4–3 shows the fields for the XML format.

Example 4–3 XML Format of Alerts

```
<EMAlert>
  <AlertGuid/>
  <ExternalAlertId/>
  <ViolationId/>
  <TargetType/>
  <TargetName/>
  <MetricName/>
  <MetricColumn/>
  <KeyValues/>
  <Message/>
  <Severity/>
  <SeverityCode/>
```

```
  <CollectionTime/>
  <AlertPageURL/>
  <EMUser/>
  <NotificationRuleName/>
  <TargetHost/>
  <TargetTimezone/>
  <Property>
    <Name/>
    <Value/>
  </Property>
</EMAlert>
```

Table 4–3 provides a description of the fields shown in Example 4–3.

Table 4–3 Field Descriptions for XML Format

Field	Description
AlertGuid	Unique identifier of the alert in Oracle Enterprise Manager.
ExternalAlertId	Unique identifier of the alert in Microsoft SCOM. This will only be set for updates.
CollectionTime	Time the alert was generated.
TargetType	Target type for which the alert was generated.
TargetName	Target name that is a unique instance of the target type.
MetricName	Name of the metric that was violated.
MetricColumn	Column under the metric that was violated.
KeyValues	Key values associated with the metric column that was violated.
Severity	Severity text assigned to the alert.
SeverityCode	Severity numeric code assigned to the alert.
EMUser	User that owns the rule that generated the alert.
NotificationRuleName	Name of the notification rule that caused the alert to be forwarded to Microsoft SCOM.
AlertPageURL	Link to the web page for the alert.
Message	Description of the alert.
TargetHost	Host name of the system where the target resides.
TargetTimezone	Time zone of the system where the target resides.
Property	Additional properties that do not have a specific field in the alert model.

4.1.3 Changing a Mapping

This section explains how to customize the mapping between Enterprise Manager and the Microsoft SCOM web service. The procedure provides the steps required for changing a mapping. Following this procedure, an example is provided that shows how to change the mapping of the target type and target name fields.

1. Study the default mapping and determine the changes you want to make. See Appendix A for details about the default mappings and the files that define the mapping for the different Enterprise Manager operations.

2. Create a back-up copy of the XSL file you want to change.
3. Open the XSL file in a text editor or in an XSLT editor.
4. Change the file to map the fields as determined in step 1. You might need to study the information in Section 4.1.1 and Section 4.1.2. These sections describe the data formats of the Microsoft SCOM alerts and Oracle Enterprise Manager alerts.
5. Save your changes.

The files are now ready for integration. You do not need to stop and start OMS. The changes will automatically be picked up.

Example of Changing a Mapping

By default, the alert name in the Microsoft SCOM alert is set to the Oracle Enterprise Manager metric column, and no custom fields are mapped. The following example shows how to change the alert name and add mappings for custom fields. The changes made to the default mapping are:

- The alert name is modified to use a hard-coded value of Alert From Oracle Enterprise Manager.
- Custom field 1 is set to the Target Type.
- Custom field 2 is set to the Target Name.
- Custom field 3 is set to the Metric Name.
- Custom field 4 is set to the Metric Column.

1. Make a back-up copy of the `createalert_request.xsl` file and name it `default_createalert_request.xsl`.
2. Make a backup copy of the `updatealert_request.xsl` file and name it `default_updatealert_request.xsl`.
3. Open the `createalert_request.xsl` file in your text editor.
4. Change the appropriate sections to reflect the new mapping.
   - **Before Changes**

     The code below shows the impacted sections in the file before the changes.

```
<xsl:value-of select="a:MetricColumn"/>
    </summary>
    ...
    <extended-fields>
      <!-- SCOM alert custom fields -->
      <!-- Uncomment fields to be set and replace "VALUE" with the actual
       value -->
      <!--
      <string-field name="CustomField1">VALUE</string-field>
      <string-field name="CustomField2">VALUE</string-field>
      <string-field name="CustomField3">VALUE</string-field>
      <string-field name="CustomField4">VALUE</string-field>
      <string-field name="CustomField5">VALUE</string-field>
      <string-field name="CustomField6">VALUE</string-field>
      <string-field name="CustomField7">VALUE</string-field>
      <string-field name="CustomField8">VALUE</string-field>
      <string-field name="CustomField9">VALUE</string-field>
      <string-field name="CustomField10">VALUE</string-field>
      -->
    </extended-fields>
```

- **After Changes**

  The code below shows the Extended Fields section in the file after the changes. The changes are shown in bold.

```
<!-- SCOM alert title -->
     <summary>
    <!-- SCOM alert title -->
     <summary>
        Alert From Oracle Enterprise Manager
     </summary>
     ...
     <extended-fields>
       <!-- SCOM alert custom fields -->
       <!-- Uncomment fields to be set and replace "VALUE" with the actual
        value -->
       <string-field name="CustomField1">
         <xsl:value-of select="a:TargetType"/>
       </string-field>
       <string-field name="CustomField2">
         <xsl:value-of select="a:TargetName"/>
       </string-field>
       <string-field name="CustomField3">
         <xsl:value-of select="a:MetricName"/>
       </string-field>
       <string-field name="CustomField4">
         <xsl:value-of select="a:MetricColumn"/>
       </string-field>
       <!--
       <string-field name="CustomField5">VALUE</string-field>
       <string-field name="CustomField6">VALUE</string-field>
       <string-field name="CustomField7">VALUE</string-field>
       <string-field name="CustomField8">VALUE</string-field>
       <string-field name="CustomField9">VALUE</string-field>
       <string-field name="CustomField10">VALUE</string-field>
       -->
     </extended-fields>
```

5. Save your changes after making the updates.
6. Open the `updateAlert_request.xsl` file and make the same changes for the custom fields. In this case, you cannot set the alert name because it is only valid for creates.
7. Save your changes after making the updates.

4.2 Changing Default Port Numbers

In most cases, you can use the default port numbers that the Microsoft SCOM web service uses. However, if there are any conflicts with existing applications, you need to change the port numbers.

8080 is the default port number for HTTP communication, and 8443 is the default port for HTTPS communication. To change the port number, perform the following steps on the system where the Microsoft SCOM web services are installed. Replace `<SCOMWS_INSTALL>` with the directory where the Microsoft SCOM web services are installed.

1. Open a command prompt window and change the working directory to:

   `<SCOMWS_INSTALL>\adapters\conf`

2. Make a backup copy of the framework.properties file.
3. Enter the following command to configure the web service to connect to the Microsoft SCOM Agent...

   ```
   ..\bin\propertiesEditor.bat -p
   services.url=<prot>://localhost:<newPort>/
   services framework.properties
   ```

   ... where `<prot>` is the protocol (HTTPS or HTTPS) and `<newPort>` is the new port number.

   The `propertiesEditor.bat` script is specifically for the Windows platform. The equivalent script for Unix platforms is `propertiesEditor.sh`.
4. Change the working directory to `..\bin`.
5. Enter the following command to restart the Microsoft SCOM web service.
   - If the web service is installed on a Unix system:

     ```
     ./service.sh restart
     ```
   - If the web service is installed on a Windows system as a standalone application, close the window where the adapter was running, then run:

     ```
     startAdapters.bat
     ```
   - If the web service is installed on a Windows system as a Windows service, enter the following commands:

     ```
     net stop iWaveAdapters
     ```

     ```
     net start iWaveAdapters
     ```

Perform the following steps to change the URL the SCOM connector is using:

1. Log in to the Oracle Enterprise Manager console by entering a user name with a 'Super Administrator' role, entering the appropriate password, then clicking **Login**.
2. Click the **Setup** link at the top right part of the window. The Overview of Setup page appears.
3. Click the **Management Connectors** link on the left side of the window. The Management Connectors page appears, which shows the installed connectors.
4. Click on the **Configure** icon associated with the SCOM Connector. This invokes edit mode, enabling you to configure the connector.
5. Change the URLs listed in the Web Service End Points section to use the new port number.
6. Click **OK** to save your changes.

4.3 Changing the Default Custom Field

The SCOM Agent requires that a custom field be set aside for its exclusive use. By default, alerts that the SCOM Agent creates will have custom field 10 set to the Guid of the event that triggered the alert. If this presents a problem, perform the following steps to change the SCOM Agent to use a different custom field.

1. Change the OracleEnterpriseManager.Alert.Creator.xml management pack file to place the event Guid in a different custom field:

a. On the system where the SCOM Agent is installed, navigate to the directory where the OracleEnterpriseManager.Alert.Creator.xml file is located.

b. Open the file with a text editor and search for Custom10. You should find the following line in the file:

```
<Custom10>$Data/EventOriginId$</Custom10>
```

c. Change "`$Data/EventOriginId$`" to "`$Data/Params/Param[20]$`".

d. Locate the tag for the custom field that the SCOM Agent will use, and change the contents to "`$Data/EventOriginId$`".

e. Save the file and exit the editor.

2. Import the updated management pack into SCOM as described in Installing the Alert Creator Management Pack on page 2-5.

3. Change the SCOM Web Service configuration to search for the event Guid in a different custom field:

a. On the system where the SCOM Web Service is installed, navigate to the `adapters/conf` directory in the SCOM Web Service installation directory.

b. Open the framework.properties file with a text editor and search for the `scom2007.connector.response.query` property.

c. Change CustomField10 in the search string to the custom field number the management pack is setting.

d. Save the file and exit the editor.

4. Stop and start the SCOM Web Service.

Refer to the appropriate section in Chapter 2 based on the platform where the SCOM Web Service is installed. For Unix platforms, see Running the Web Service on Unix on page 2-8. For Windows platforms, see Running the Web Service on Windows on page 2-10.

4.4 Changing SCOM API Connection Parameters

When installing the SCOM Agent, you must configure the connection parameters used for accessing the SCOM API. The installation includes the SCOMAgentConfig utility you can use to change the Agent configuration parameters.

Perform the following steps to change the connection parameters:

1. Open Windows Explorer on the system where the SCOM Agent is installed.
2. Navigate to the bin directory in the SCOM Agent installation directory.
3. Run the `SCOMAgentConfig.exe` utility. This action starts the SCOM Agent Configuration Tool.
4. Click **Load**. This action opens a directory navigation window.
5. Navigate to the SCOM Agent installation directory and open the SCOMAgent.cfg file.
6. Click the **Management Groups** tab and click **Edit**. This action displays the Edit Management Group window.
7. Change the desired information in the following fields listed, then click **Update**:

Name
Server

Domain
Username
Password

8. Click **Save** to save the changes to the configuration file.
9. Click **Exit** to exit the utility.
10. Stop and restart the SCOM Agent in IIS.

5

Troubleshooting the Connector

This chapter provides information to assist in troubleshooting integration issues with Microsoft SCOM. The chapter focuses on troubleshooting issues in the web service front-end and the back-end Agent.

This chapter discusses the following topics:

5.1 Preparing for Troubleshooting

In order to troubleshoot integration issues, you must adjust the Oracle Enterprise Manager logging options to capture additional information.

To enable debug logging information:

1. Edit the `emomslogging.properties` file using a text editor. The file is located in the following directory ...

   11.1.0.1

   `<ORACLE_HOME>/oms11g/sysman/config`

   10.2.0.5

   `<ORACLE_HOME>/oms10g/sysman/config`

   ... where `<ORACLE_HOME>` is the Oracle installation directory.

2. Set the parameters as follows:

   ```
   log4j.appender.emlogAppender.Threshold = DEBUG
   log4j.rootCategory=DEBUG, emlogAppender, emtrcAppender
   ```

3. After setting the debug logging parameters, restart OMS by opening a command window, changing the working directory to `<ORACLE_HOME>/oms10g/bin`, and issuing the following commands:

   ```
   emctl stop oms
   emctl start oms
   ```

5.2 Using the Correct URL for SCOM Web Service Operations

Perform the following steps to identify and configure the connector to use the correct URL for SCOM Web Service operations.

1. Open a command terminal on the system where the SCOM web service is installed.
2. Change the working directory to the `adapters/log` directory in the SCOM web service installation directory.
3. Open the framework.log file in a text editor.
4. Go to the bottom of the file and search backwards for the string “Setting the server's publish address to be”. Continue searching backwards until you find the URL that contains `/AcquisitionService`.

   You should specify the URL listed here for the `getNewAlerts`, `getUpdatedAlerts`, and `acknowledgeAlerts` operations, with one exception. You must replace the host name of `localhost` in the URL with the actual host name or IP address of the system where the SCOM Web Service is installed.
5. Go to the bottom of the file and search backwards for the string “Setting the server's publish address to be." Continue searching backwards until you find the URL that contains EventService.

   You should specify the URL listed here for the createalert and updatealert operations, with one exception. You must replace the host name of localhost in the URL with the actual host name or IP address of the system where the SCOM Web Service is installed.
6. Go to the bottom of the file and search backwards for the string “Setting the server's publish address to be". Continue searching backwards until you find the URL that contains SCOMService.

   You should specify the URL listed here for the setup and cleanup operations, with one exception.You must replace the host name of localhost in the URL with the actual host name or IP address of the system where the SCOM Web Service is installed.
7. Log in to the Oracle Enterprise Manager console by entering a user name with a ‘Super Administrator’ role, entering the appropriate password, then clicking **Login**.
8. Click the **Setup** link at the top right part of the window. The Overview of Setup page appears.
9. Click the **Management Connectors** link on the left side of the window. The Management Connectors page appears, which shows the installed connectors.
10. Click on the **Configure** icon associated with the SCOM Connector. This invokes edit mode, enabling you to configure the connector.
11. Verify that the URL identified in step 4 is specified for the getNewAlerts, getUpdatedAlerts, and acknowledgeAlerts operations.
12. Verify that the URL identified in step 5 is specified for the createalert and updatealert operations.
13. Verify that the URL identified in step 6 is specified for the setup and cleanup operations.
14. If any of the operations are incorrect, change to the correct URL and click **OK**.

5.3 Diagnosing Problems with Alert Generation and Updates

You might encounter issues involved in generating or updating alerts in SCOM from alerts that have originated in Oracle Enterprise Manager or vice versa. The following sections provide diagnostic information to resolve these problems.

5.3.1 Alerts from Oracle Enterprise Manager to SCOM

SCOM can generate or update alerts from alerts that have originated in Oracle Enterprise Manager. Perform the following diagnostic steps if SCOM alerts are not being generated or updated as expected.

1. Verify that a notification rule is set up for the condition that triggered the alert. Perform the following steps to verify that it is set up correctly:
   a. Open an Oracle Enterprise Manager console window and log in.
   b. Click on the **Setup** link in the upper right corner of the Oracle Enterprise Manager console.
   c. Click on the **Notification Methods** link on the left side of the window.
   d. Locate the SCOM Connector in the table near the bottom of the window and click on it to list and note the notification rules that use this method.
   e. Click on the **Preferences** link in the upper right corner.
   f. Click on the **Notification Rules** link on the left side of the window. This displays a list of all defined notification methods.
   g. Examine the details for the rules listed in step d above and verify that at least one rule matches the conditions that triggered the alert.
   h. If you did not find at least one rule, you need to modify an existing notification rule or add a new one to invoke the SCOM notification method.
2. Verify that the OracleEnterpriseManager.Alert.Creator Management Pack has been imported into the SCOM server:
   a. Open the Ops Mgr 2007 console window and log in.
   b. In the Administration pane of the OpsMgr console, select **Administration**, then **Management Packs**.
   c. Verify that the "OracleEnterpriseManager Alert Creator" Management Pack is listed.
   d. If the pack is not listed, import it as specified in Installing the Alert Creator Management Pack on page 2-5.
3. Determine the error that Oracle Enterprise Manager has reported.
   a. Navigate to the page that displays the alert information that should have triggered the new alert in SCOM.

      For example, if the Memory Utilization % metric was set up to invoke the SCOM Connector method, you would perform the following steps to access the page that displays alert information. This example assumes that the generated alert was critical.

      1.) Click on the **Alerts** tab.

      2.) Click on the **Critical** sub-tab.

      3.) Click on the **Memory Utilization** % alert.

b. Click on the details and look for any error alerts.

After the alert is generated, it initially indicates that the method will be invoked, but no error alerts appear. The Enterprise Manager Connector Framework makes several attempts to transfer the alert information to the SCOM web service. After all attempts have failed, an error alert is usually added to the details for the alert. If there are no errors after several minutes, it is likely that no error alerts will be added to the log.

c. If there is no error information in the alert details, you need to examine the log file for errors. Perform the following steps to locate errors in the log file:

1.) Open the emoms.trc file in a text editor. The location of the file depends on the EM version. For 11.1.0.1, the file is located at:

```
<EM_INSTANCE_BASE>/em/<OMS_NAME>/sysman/log
```

... where `<EM_INSTANCE_BASE>` is the OMS Instance Base directory. By default, the OMS Instance Base directory is `gc_inst`, which is present under the parent directory of the Oracle Middleware Home.

For 10.2.0.5, the file is located in `$OMS_HOME/sysman/log`.

2.) Go to the bottom of the file and search backwards for this string:

```
ERROR core.EMEventConnectorServiceImpl createEvent
```

The error alert is contained in the Exception information.

4. Diagnose the problem based on the error alert. See Section 5.4, "Resolving Alerts from Oracle Enterprise Manager" for information on troubleshooting common error alerts.

5.3.2 Alerts from SCOM to Oracle Enterprise Manager

Oracle Enterprise Manager can generate or update alerts resulting from alerts that have originated in SCOM. Perform the following diagnostic steps if SCOM alerts are not being generated or updated as expected.

1. Verify that the SCOM Agent has a subscription in SCOM:

a. In the Administration pane of the SCOM console, select **Administration**, then **Notification**, then **Product Connectors**. The SCOM Agent should be listed as a product connector.

b. Right-click on the SCOM Agent and select **Properties** from the list of options. The SCOM Agent – Product Connector Properties window appears.

c. Check whether a subscription is listed in the Subscriptions section.

If a subscription is listed, select the subscription and click **Edit**.

If a subscription is not listed, add a subscription as described in Adding a Subscription in SCOM on page 3-4.

d. Check the subscription and make sure it is configured as specified in Adding a Subscription in SCOM on page 3-4.

2. Verify that no other connectors are subscribed to the same alert information. If there are, contact Microsoft support for resolution.

3. Determine the error that Oracle Enterprise Manager has reported:

a. Open the `emoms.trc` file in a text editor. The location of the file depends on the EM version. For 11.1.0.1, the file is located at:

```
<EM_INSTANCE_BASE>/em/<OMS_NAME>/sysman/log
```

... where `<EM_INSTANCE_BASE>` is the OMS Instance Base directory. By default, the OMS Instance Base directory is `gc_inst`, which is present under the parent directory of the Oracle Middleware Home.

For 10.2.0.5, the file is located in `$OMS_HOME/sysman/log`.

b. Go to the bottom of the file and search backwards for `getNewAlerts()`.

See Section 5.5, "Resolving Alerts from SCOM" for the error alert you found in the log file. Each alert entry explains the cause of the problem and the steps required to correct the problem.

5.4 Resolving Alerts from Oracle Enterprise Manager

This section provides cause and solution information on troubleshooting common alert messages. Find the error message in Table 5–1 that matches your alert message, then refer to the corresponding section(s) indicated under Possible Cause for instructions to diagnose and correct the problem.

Table 5–1 Enterprise Manager Alert Messages

Alert Message	Possible Cause	Applicable Versions
targetException=oracle.xml.parser.v2.XMLParseException: Start of root element expected	Invalid Web Service Credentials	10.2.0.4, 10.2.0.5
javax.net.ssl.SSLException: SSL handshake failed: X509CertChainInvalidErr	SSL Not Configured in Enterprise Manager	10.2.0.4, 10.2.0.5
The wallet "/gc/OracleHomes/oms10g/sysman/connector//certdb.txt" does not exist	Missing certdb.txt File	10.2.0.4, 10.2.0.5
Error opening socket: java.net.ConnectException: Connection refused	SCOM Web Service Down	10.2.0.4, 10.2.0.5
java.lang.Exception: Error occurred while calling Web Service:	Invalid XML Format	10.2.0.4, 10.2.0.5
Error opening socket: java.net.UnknownHostException: <hostname>	Unknown Host	10.2.0.4, 10.2.0.5
Error opening socket: java.net.NoRouteToHostException: No route to host	Invalid IP Address or Port Number	10.2.0.4, 10.2.0.5
SOAPException: faultCode=SOAP-ENV:Protocol; msg=Unsupported response content type "text/html;	Invalid URL Path	10.2.0.4, 10.2.0.5
ERROR: could not connect to the server <hostname> because it is not operational	SCOM Server Not Operational	10.2.0.4, 10.2.0.5, 11.1.0.1
ERROR - Could not log in to the server because the password is invalid	Invalid SCOM API Credentials	10.2.0.4, 10.2.0.5, 11.1.0.1
Microsoft.EnterpriseManagement.Common.UnauthorizedAccessMonitoringException: The user <Domain>\<Username> does not have sufficient permission to perform the operation	Wrong SCOM API Permissions	10.2.0.4, 10.2.0.5, 11.1.0.1
ERROR occurred invoking SCOM connector to insert event for null	SCOM Agent Not Operational	10.2.0.4, 10.2.0.5, 11.1.0.1
javax.xml.ws.WebServiceException: org.apache.cxf.service.factory.ServiceConstructionException: Failed to create service	SCOM Agent Configuration	10.2.0.4, 10.2.0.5, 11.1.0.1

Table 5–1 (Cont.) Enterprise Manager Alert Messages

Alert Message	Possible Cause	Applicable Versions
Request failed because the specified management pack could not be found	Management Pack Missing	10.2.0.4, 10.2.0.5, 11.1.0.1
Successfully inserted the event, but timed out waiting for the alert to be created	Alert Create Timeout	10.2.0.4, 10.2.0.5, 11.1.0.1
The server sent HTTP status code 403: Forbidden	Invalid Web Service Credentials	11.1.0.1
javax.net.ssl.SSLKeyException: [Security:090477]Certificate chain received from <hostname> - <IPAddress> was not trusted causing SSL handshake failure	SSL Not Configured in Oracle Wallet Manager, Missing certdb.txt File	11.1.0.1
HTTP transport error: java.net.SocketException: Socket Closed	SCOM Web Service Down, Invalid IP Address or Port Number	11.1.0.1
HTTP transport error: java.net.UnknownHostException: <hostname>	Unknown Host	11.1.0.1
The server sent HTTP status code 404: Not Found	Invalid URL Path	11.1.0.1

Invalid Web Service Credentials

Cause

The user name or password for accessing the SCOM web service is incorrect.

Solution

1. Log in to the Oracle Enterprise Manager console by entering a user name with a 'Super Administrator' role, entering the appropriate password, then clicking **Login**.
2. Click the **Setup** link at the top right corner of the window. The Overview of Setup page appears.
3. Click the **Management Connectors** link on the left side of the window. The Management Connectors page appears, which shows the installed connectors.
4. Click on the **Configure** icon associated with the SCOM Connector.
5. Click the **General** tab.
6. Correct the SCOM Web Service Username and SCOM Web Service Password fields, then click **OK**.

SSL Not Configured in Oracle Wallet Manager

Cause

The SSL handshake between the Oracle Enterprise Manager Connector Framework and the SCOM web service failed. This failure occurs because Oracle Enterprise Manager is not configured correctly with the SSL certificate for the SCOM web service. The SSL certificate the SCOM web service uses must be imported into the wallet manager. The certificate is either missing from the wallet or does not match the SSL certificate provided by the SCOM web service.

Solution

Import the SSL certificate from the SCOM web service into the wallet manager. See Section 2.3.3.1, "Adding Signed Certificates to Wallet Manager" for details on setting up Oracle Enterprise Manager with the SCOM SSL certificate.

Missing certdb.txt File

Cause

The SCOM web service is configured to use SSL, but the certdb.txt file that contains the SSL information is missing.

Solution

Import the SSL certificate from the SCOM web service into the wallet manager. See Section 2.3.3.1, "Adding Signed Certificates to Wallet Manager" for details on setting up Oracle Enterprise Manager with the SCOM SSL certificate.

SCOM Web Service Down

Cause

The SCOM web service is down.

Solution

Perform the following steps to check the status of the web service and start it if necessary.

If the SCOM web service is installed on a Unix system:

1. Open a command terminal on the system where the SCOM web service is installed.
2. Change the working directory to the `adapters/bin` directory in the SCOM web service installation directory.
3. Enter the following command:

   ```
   ./service.sh status
   ```

4. If the command indicates that the service is not running, enter the following command:

   ```
   ./service.sh start
   ```

If the SCOM web service is installed on a Windows system:

1. Open a command terminal on the system where the SCOM web service is installed.
2. Change the working directory to the adapters/log directory in the SCOM web service installation directory.
3. Open the framework.log file in a text editor.
4. Go to the bottom of the file and search backwards for the string iWave Adapter Framework. If the last occurrence found is iWave Adapter Framework Started, this indicates that the web service is started.
5. If the web service is not started, start the web service based on how the web service is installed.
   - If it is installed as a standalone application, change the working directory to the adapters/bin directory and run the startAdapters.bat command file.

- If it is installed as a Windows service, enter the net start iWaveAdapters command.

Invalid XML Format

Cause

The request sent to the SCOM web service was rejected because the XML was formatted incorrectly. This problem should not occur unless the connector configuration XML files are manually updated.

Solution

Look at the error alert in the fault string node of the SOAP fault response and determine what is incorrect in the request document. Examine any changes made to the XML configuration files for mistakes that could have caused the problem. You can determine the correct XML format by accessing the WSDL using a web browser.

Perform the following steps to access the WSDL:

1. Log in to the Oracle Enterprise Manager console by entering a user name with a 'Super Administrator' role, entering the appropriate password, then clicking **Login**.
2. Click the **Setup** link at the top right corner of the window. The Overview of Setup page appears.
3. Click the **Management Connectors** link on the left side of the window. The Management Connectors page appears, which shows the installed connectors.
4. Click on the **Configure** icon associated with the SCOM Connector.
5. Click the **General** tab.
6. Select and copy the URL specified for the getNewAlerts operation.
7. Open an internet browser on the system where the Oracle Enterprise Manager server is installed.
8. In the address window, enter the URL that was copied in step 6 above. Add ?wsdl to the end of the URL. The URL should appear similar to the following example:

   ```
   http://[Hostname]:8080/services/SCOM2007/EventService?wsdl
   ```

   `[Hostname]` is the actual host name or IP address where the SCOM web service is installed.

If you cannot determine why the format is incorrect, contact Oracle for support.

Unknown Host

Cause

The system does not recognize the host name specified in the URL.

Solution

You can use the following options to address this issue:

- Coordinate with the system administrator to change the system configuration to recognize the host name.
- Specify the IP address in the URL instead of the host name. To do this, perform the following steps:

1. Determine the IP address of the system where the SCOM web service is installed.
2. Log in to the Oracle Enterprise Manager console by entering a user name with a 'Super Administrator' role, entering the appropriate password, then clicking **Login**.
3. Click the **Setup** link at the top right part of the window. The Overview of Setup page appears.
4. Click the **Management Connectors** link on the left side of the window. The Management Connectors page appears, which shows the installed connectors.
5. Click on the **Configure** icon associated with the Microsoft SCOM Connector. This invokes edit mode, enabling you to configure the connector.
6. Change the host name to the IP address in the URL specified for the createalert and updatealert operations.
7. Click **OK**.

Invalid IP Address or Port Number

Cause

The IP address or port number specified in the URL is invalid, or the network is down.

Solution

Verify that the hostname/IP address configured for the connector is correct:

1. Log in to the Oracle Enterprise Manager console by entering a user name with a 'Super Administrator' role, entering the appropriate password, then clicking **Login**.
2. Click the **Setup** link at the top right part of the window. The Overview of Setup page appears.
3. Click the **Management Connectors** link on the left side of the window. The Management Connectors page appears, which shows the installed connectors.
4. Click on the **Configure** icon associated with the SCOM Connector. This invokes edit mode, enabling you to configure the connector.
5. Verify that the hostname/IP address and port number specified in the URL for the createalert and updatealert operations are correct.
6. If the hostname/IP address and port number are incorrect, provide the correct values and click **OK**.

If the URLs specify a host name, make sure that the host name resolves to the correct IP address. To determine the IP address of the host name, issue the ping `<hostname>` command, where `<hostname>` is the actual host name. This lists the IP address that was resolved for the host name. If this is incorrect, the system administrator needs to investigate why it is incorrect. If the ping fails, the system administrator needs to investigate why there is no connectivity.

Invalid URL Path

Cause

The web service received the request and rejected it because there was a problem. This likely indicates that an invalid path was specified in the URL.

Solution

To determine the reason for the failure, examine the HTML document listed with the Exception information in the emoms.trc log file. In the HTML document, it provides error information that indicates the reason why it was rejected. The error information may be difficult to spot because the HTML tag delimiters are encoded.

If the error information specifies “HTTP Error: 404”, this indicates that the path in the URL is incorrect. Perform the following steps to test the URL the connector is using.

1. Log in to the Oracle Enterprise Manager console by entering a user name with a ‘Super Administrator’ role, entering the appropriate password, then clicking **Login**.
2. Click the **Setup** link at the top right part of the window. The Overview of Setup page appears.
3. Click the **Management Connectors** link on the left side of the window. The Management Connectors page appears, which shows the installed connectors.
4. Click on the **Configure** icon associated with the SCOM Connector.
5. Click the **General** tab.
6. Select and copy the URL specified for the createalert operation.
7. Open an internet browser on the system where the Oracle Enterprise Manager server is installed.
8. In the address window, enter the URL that was copied in step 6 above. Add ?wsdl to the end of the URL. The URL should appear similar to the following example:

   `http://[Hostname]:8080/services/SCOM2007/EventService?wsdl`

   `[Hostname]` is the actual host name or IP address where the SCOM web service is installed.

If the WSDL is loaded, this confirms that the URL is correct. If it fails to load, there is a problem with the URL. Perform the steps specified in Section 5.2, "Using the Correct URL for SCOM Web Service Operations" to configure the connector to use the correct URL.

SCOM Server Not Operational

Cause

The SCOM Agent could not insert the alert into SCOM because the wrong host name is configured for SCOM or the SCOM server is down.

Solution

Perform the following steps to determine and correct the root cause of the problem:

1. Verify that the host name or IP address listed in the error message is correct for the RMS system. If the host name or IP address are incorrect, perform the following steps to correct the configuration:
   a. Open Windows Explorer on the system where the SCOM Agent is located.
   b. Navigate to the bin directory in the SCOM Agent installation directory.

c. Run the SCOMAgentConfig.exe utility to start the SCOM Agent Configuration Tool.

d. Click **Load** to open a directory navigation window.

e. Navigate to the SCOM Agent installation directory and open the SCOMAgent.cfg file.

f. Click the **Management Groups** tab, then click **Edit** to display the Edit Management Group window.

g. Correct the hostname/IP address in the Server field, then click **Update**.

h. Click **Save** to save the changes to the configuration file.

i. Click **Exit** to exit the utility.

j. Stop and restart the SCOM Agent in IIS.

2. Verify that the following OpsMgr services are running:

   OpsMgr Config Service
   OpsMgr Health Service
   OpsMgr SDK Service

Invalid SCOM API Credentials

Cause

The SCOM Agent could not send the alert to the SCOM server, because the credentials configured for accessing the SCOM API are invalid.

Solution

Perform the following steps to change the credentials for accessing the SCOM API:

1. Open Windows Explorer on the system where the SCOM Agent is located.
2. Navigate to the bin directory in the SCOM Agent installation directory.
3. Run the SCOMAgentConfig.exe utility to start the SCOM Agent Configuration Tool.
4. Click **Load** to open a directory navigation window.
5. Navigate to the SCOM Agent installation directory and open the SCOMAgent.cfg file.
6. Click the **Management Groups** tab, then click **Edit** to display the Edit Management Group window.
7. Correct the credential information in the Domain, Username, and Password fields, then click **Update**.
8. Click **Save** to save the changes to the configuration file.
9. Click **Exit** to exit the utility.
10. Stop and restart the SCOM Agent in IIS.

Wrong SCOM API Permissions

Cause

The SCOM Agent could not send the alert to the SCOM server, because the credentials configured for accessing the SCOM API do not have sufficient permissions.

Solution

Refer to Setting Up the Agent Account on page 2-2. This section provides the steps required to set up the account for accessing the SCOM API.

SCOM Agent Not Operational

Cause

The web service could not create an alert in SCOM because the SCOM Agent is not operational.

Solution

Open IIS Manager on the system where the SCOM Agent was installed, and start the web site for the Agent.

SCOM Agent Configuration

Cause

The web service could not connect to the SCOM Agent because the web service has an invalid configuration parameter. Either the URL for the SCOM Agent is incorrect or the credentials for accessing the SCOM Agent are invalid.

Solution

1. Verify that the URL for the SCOM Agent is correct. You should specify the the URL that was provided at the end of the SCOM Agent installation. Note that if the host name in the URL is localhost and you are accessing it from another system, you need to replace localhost with the host name or IP address of the SCOM Agent installation machine.

   If you do not know the URL, you can determine it as follows:

   - If the SCOM Agent was installed as a web site, the address is:

     `http://<IP>:<port>/Service.asmx`

     ... where `<IP>` is the IP address, and <port> is the port number specified when installing the Agent.

   - If the SCOM Agent was installed as a virtual directory, the address is:

     `http://<IP>:<port>/<vdir>/Service.asmx`

     ... where `<IP>` is the IP address, `<port>` is the port number for the web service where the agent was installed, and `<vdir>` is the virtual directory name specified for the Agent.

2. Select a user name and password that are valid on the system where the SCOM Agent was installed.
3. Open a command window and change the working directory to `adapters\endpoints\SCOM2007` in the SCOM web service installation directory.
4. Rerun the SCOM Web Service installer using the URL and credentials from the preceding steps. See Section 2.3.1.1, "Installing the Web Service on Unix" or Section 2.3.2.1, "Installing the Web Service on Windows", depending on your platform, for the procedure.

Management Pack Missing

Cause

The web service could not create an alert in SCOM because the OracleEnterpriseManager.Alert.Creator management pack has not been imported into SCOM.

Solution

Refer to Installing the Alert Creator Management Pack on page 2-5 for the steps required to import the management pack into SCOM.

Alert Create Timeout

Cause

The web service was able to insert an event in SCOM, but an alert was not created within the timeout period. This likely indicates that an error occurred in the alert generating rule and it was unloaded by SCOM. Whenever this occurs, the Ops Mgr Health Service generates an error followed by a warning in the Operations Manager log. The error entry begins with the following message:

```
A module reported an error 0x80070057 from a callback which was running as part of
rule "Create.Default.Alert" running for instance "OracleEnterpriseManager Event
Source" with id ...
```

The warning entry begins with the following message:

```
Summary: 1 rule(s)/monitor(s) failed and got unloaded, 1 of them reached the
failure limit that prevents automatic reload ...
```

> **Note:** This situation should not occur if the default SCOM connector configuration files are used. The only known way this can occur is if the SCOM Agent web service is directly accessed and an invalid value is passed for the Priority or Severity fields.

Solution

Restart the Windows service named “Ops Mgr Health Service” on the RMS system.

5.5 Resolving Alerts from SCOM

This section provides cause and solution information on troubleshooting common alert messages. Find the error message in Table 5–2 that matches your error message, then refer to the corresponding section(s) indicated under Possible Cause for instructions to diagnos and correct the problem.

Table 5–2 SCOM Error Messages

Error Message	Possible Cause	Applicable Versions
targetException=oracle.xml.parser.v2.XMLParseException: Start of root element expected.	Invalid Web Service Credentials	10.2.0.4, 10.2.0.5
SOAPException: faultCode=SOAP-ENV:IOException; msg=javax.net.ssl.SSLException: SSL handshake failed: X509CertChainInvalidErr	SSL Not Configured in Enterprise Manager	10.2.0.4, 10.2.0.5
SOAPException: faultCode=SOAP-ENV:IOException; msg=The wallet "/gc/OracleHomes/oms10g/sysman/connector//certdb.txt" does not exist	Missing certdb.txt File	10.2.0.4, 10.2.0.5
SOAPException: faultCode=SOAP-ENV:Client; msg=Error opening socket: java.net.ConnectException: Connection refused;	SCOM Web Service Down, Invalid Port Number	10.2.0.4, 10.2.0.5
SOAPException: faultCode=SOAP-ENV:Client; msg=Error opening socket: java.net.UnknownHostException: <hostname>;	Unknown Host	10.2.0.4, 10.2.0.5
SOAPException: faultCode=SOAP-ENV:Client; msg=Error opening socket: java.net.NoRouteToHostException: No route to host;	Invalid IP Address	10.2.0.4, 10.2.0.5
SOAPException: faultCode=SOAP-ENV:Protocol; msg=Unsupported response content type	Invalid URL Path	10.2.0.4, 10.2.0.5
The server sent HTTP status code 403: Forbidden	Invalid Web Service Credentials	10.2.0.4, 10.2.0.5
Certificate chain received from <hostname> - <IPAddress> was not trusted causing SSL handshake failure.	SSL Not Configured in Oracle Wallet Manager, Missing certdb.txt File	11.1.0.1
Tried all: 1 addresses, but could not connect over HTTPS to server: <IPAddress> port: <port>	SCOM Web Service Down	11.1.0.1
HTTP transport error: java.net.SocketException: Socket Closed	Invalid Port Number, Invalid IP Address	11.1.0.1
HTTP transport error: java.net.UnknownHostException: <hostname>	Unknown Host	11.1.0.1
The server sent HTTP status code 404: Not Found	Invalid URL Path	11.1.0.1

Invalid Web Service Credentials

Cause

The user name or password for accessing the SCOM web service is incorrect.

Solution

1. Log in to the Oracle Enterprise Manager console by entering a user name with a 'Super Administrator' role, entering the appropriate password, then clicking **Login**.
2. Click the **Setup** link at the top right part of the window. The Overview of Setup page appears.
3. Click the **Management Connectors** link on the left side of the window. The Management Connectors page appears, which shows the installed connectors.
4. Click on the **Configure** icon associated with the SCOM Connector.

5. Click the **General** tab.
6. Correct the SCOM Web Service Username and SCOM Web Service Password fields and click **OK**.

SSL Not Configured in Oracle Wallet Manager

Cause

The SSL handshake between the Oracle Enterprise Manager Connector Framework and the SCOM web service failed. This failure occurs when the SSL certificate in the wallet manager does not match the SSL certificate that the SCOM web service provides.

Solution

You need to import the SSL certificate from the SCOM web service into the wallet manager. See Section 2.3.3.1, "Adding Signed Certificates to Wallet Manager" for details on setting up Oracle Enterprise Manager with the SCOM SSL certificate.

Missing certdb.txt File

Cause

The SCOM web service is configured to use SSL, but the `certdb.txt` file that contains the SSL information is missing.

Solution

You need to import the SSL certificate from the SCOM web service into the wallet manager. See Section 2.3.3.1, "Adding Signed Certificates to Wallet Manager" for details on setting up Oracle Enterprise Manager with the SCOM SSL certificate.

SCOM Web Service Down

Cause

The SCOM web service is down.

Solution

Perform the following steps to check the status of the web service and start it if necessary.

If the SCOM web service is installed on a Unix system:

1. Open a command terminal on the system where the SCOM web service is installed.
2. Change the working directory to the adapters/bin directory in the SCOM web service installation directory.
3. Enter the following command:

   ```
   ./service.sh status
   ```

4. If the command indicates that the service is not running, enter the following command:

   ```
   ./service.sh start
   ```

If the SCOM web service is installed on a Windows system:

1. Open a command terminal on the system where the SCOM web service is installed.
2. Change the working directory to the `adapters/log` directory in the SCOM web service installation directory.
3. Open the framework.log file in a text editor.
4. Go to the bottom of the file and search backwards for the string iWave Adapter Framework. If the last occurrence found is iWave Adapter Framework Started, this indicates that the web service is started.
5. If the web service is not started, start the web service based on how the web service is installed:
   - If it is installed as a standalone application, change the working directory to the `adapters/bin` directory and run the startAdapters.bat command file.
   - If it is installed as a Windows service, enter the net start iWaveAdapters command.

If the web service is not down, there must be a problem with the port number. Perform the steps specified in Section 5.2, "Using the Correct URL for SCOM Web Service Operations" to identify the correct URL, including the port number.

Invalid Port Number

Cause

The port number in the URL is incorrect.

Solution

Perform the steps specified in Section 5.2, "Using the Correct URL for SCOM Web Service Operations" to identify the correct URL, including the port number.

Unknown Host

Cause

The system does not recognize the host name specified in the URL.

Solution

Select one of the following options to address this issue.

- Coordinate with the system administrator to change the system configuration to recognize the host name.
- Specify the IP address in the URL instead of the host name. To do this, perform the following steps:
  1. Determine the IP address of the system where the SCOM web service is installed.
  2. Log in to the Oracle Enterprise Manager console by entering a user name with a 'Super Administrator' role, entering the appropriate password, then clicking **Login**.
  3. Click the **Setup** link at the top right part of the window. The Overview of Setup page appears.
  4. Click the **Management Connectors** link on the left side of the window. The Management Connectors page appears, which shows the installed connectors.

5. Click on the **Configure** icon associated with the SCOM Connector. This invokes edit mode, enabling you to configure the connector.
6. Change the host name to the IP address in the URL specified for the getNewAlerts, getUpdatedAlerts, and acknowledgeAlerts operations.
7. Click **OK**.

Invalid IP Address

Cause

The IP address specified in the URL is invalid, or the network is down.

Solution

Verify that the hostname/IP address configured for the connector is correct:

1. Log in to the Oracle Enterprise Manager console by entering a user name with a 'Super Administrator' role, entering the appropriate password, then clicking **Login**.
2. Click the **Setup** link at the top right part of the window. The Overview of Setup page appears.
3. Click the **Management Connectors** link on the left side of the window. The Management Connectors page appears, which shows the installed connectors.
4. Click on the **Configure** icon associated with the SCOM Connector. This invokes edit mode, enabling you to configure the connector.
5. Verify that the hostname/IP address specified in the URL for the getNewAlerts, getUpdatedAlerts, and acknowledgeAlerts operations are correct.
6. If the hostname/IP address are incorrect, provide the correct values and click **OK**.

If the URLs specify a host name, make sure that the host name resolves to the correct IP address. To determine the IP address of the host name, issue the ping `<hostname>` command, where `<hostname>` is the actual host name. This lists the IP address that was resolved for the host name. If this is incorrect, the system administrator needs to investigate why it is incorrect.

If the hostname/IP address appears to be correct, try to ping the system where the SCOM web service is installed using the hostname/IP address. If the ping fails, the system administrator needs to investigate why there is no connectivity.

Invalid URL Path

Cause

The URL hostname/IP address and port numbers are correct, but there is an invalid path.

Solution

Perform the steps specified in Section 5.2, "Using the Correct URL for SCOM Web Service Operations" to identify the correct URL, including the port number.

A

Default Mappings

This appendix describes the default mappings between the Enterprise Manager alert data fields and the Microsoft SCOM alert data fields. The data is formatted in XML, and the XSLT files transform the data from one format to another.

For information on customizing the field mappings, see Section 4.1, "Customizing Mappings".

This appendix discusses the following topics:

- Data Translation Files
- createEvent Operation
- updateEvent Operation
- getNewAlerts and getUpdatedAlerts Operations

Data Translation Files

XML Style Sheet (XSL) files contain the mappings between the two systems. These files are located in the following directory:

`$ORACLE_HOME/sysman/connector/SCOM_Connector`

Table A–1 lists the XSL files that perform the mappings and provides a summary of each.

Table A–1 XSL Files that Perform Mappings

File	Description
`createEvent_request.xsl`	Transforms the Oracle Enterprise Manager alert data to the Microsoft SCOM alert format for the createEvent operation.
`updateEvent_request.xsl`	Transforms the Oracle Enterprise Manager alert data to the Microsoft SCOM alert format for the updateEvent operation.
`getNewAlerts_response.xsl`	Transforms data in the Microsoft SCOM alert format to the Oracle Enterprise Manager alert format. This file is invoked to transform the response for the getNewAlerts poll operation.
`getUpdatedAlerts_response.xsl`	Transforms data in the Microsoft SCOM alert format to the Oracle Enterprise Manager alert format. This file is invoked to transform the response for the getUpdatedAlerts poll operation.

The following sections provide details about the default mappings in each of the files.

createEvent Operation

The Oracle Enterprise Manager Connector Framework invokes the `createEvent` operation whenever an alert is generated in Oracle Enterprise Manager and a notification rule is configured to invoke the SCOM connector. `createEvent_request.xsl` is invoked during the process to transform the data from Oracle Enterprise Manager format to SCOM alert format. Table A–2 lists the default field mappings between the Microsoft SCOM alert and the Oracle Enterprise Manager alert.

Table A–2 createalert Operation Mappings

SCOM Field	SCOM Attribute Type	Req'd?	Oracle Enterprise Manager Alert Attributes	Value
`Name`	String	Yes	Set to the Metric Column.	<MetricColumn>
`Description`	String	Yes	Values from the alert context are listed in angle brackets in the Value column.	Received alert reported by Oracle Enterprise Manager: Collection Time — <Collection Time> Target Type — <TargetType> Target Name — <TargetName> Metric Name — <MetricName> Metric Column — <MetricColumn> * Key Values — <KeyValues> Severity — <Severity> * Notification Rule — <NotificationRuleName> * URL — <EventPageURL> Message — <Message> Fields preceded with an asterisk (*) are only present if the corresponding Enterprise Manager alert field has data.
`Priority`	String	Yes	Conditional based on the Oracle Enterprise Manager severity.	Set to Low if Oracle Enterprise Manager Severity is Information. Set to Normal if Oracle Enterprise Manager Severity is Critical. Set to High for all other Oracle Enterprise Manager severity values.
`Severity`	String	Yes	Conditional based on the Oracle Enterprise Manager severity.	Set to Information if Oracle Enterprise Manager Severity is Information. Set to Error if Oracle Enterprise Manager Severity is Critical. Set to Warning for all other Oracle Enterprise Manager severity values.

updateEvent Operation

The Oracle Enterprise Manager Connector Framework invokes the `updateEvent` operation whenever an alert is generated in Oracle Enterprise Manager and a notification rule is configured to invoke the SCOM connector. `updateEvent_request.xsl` is invoked during the process to transform the data from Oracle Enterprise Manager format to SCOM alert format. Table A–3 lists the default field mappings between the Microsoft SCOM alert and the Oracle Enterprise Manager alert.

Table A–3 updateEvent Operation Mappings

SCOM Field	SCOM Attribute Type	Req'd?	Oracle Enterprise Manager Alert Attributes	Value
`Id`	String	Yes	Set to the External Event Id.	<ExternalEventId>
`Resolution State`	String	Yes	Conditional based on the Oracle Enterprise Manager severity	Set to 255 (Closed) if Oracle Enterprise Manager Severity is Clear, Unreachable End, Blackout End, Metric Error End, or End. Set to 0 (New) for all other Oracle Enterprise Manager severity values.
`Alert History`	String	No	Conditional based on the Oracle Enterprise Manager severity.	Set to " Oracle Enterprise Manager cleared alert" if Oracle Enterprise Manager severity is Clear. Set to " Oracle Enterprise Manager changed alert severity to warning" if Oracle Enterprise Manager severity is Warning. Set to " Oracle Enterprise Manager changed alert severity to critical" if Oracle Enterprise Manager severity is Critical. Not set for other Oracle Enterprise Manager severity values.

getNewAlerts and getUpdatedAlerts Operations

The Oracle Enterprise Manager Connector Framework invokes the `getNewAlerts` operation on the poll cycle interval configured for the SCOM connector. One step in the operation is to send a request to the Microsoft SCOM web service for new alerts in Microsoft SCOM. When the response comes back, the `getNewAlerts_response.xsl` file is invoked to transform the Microsoft SCOM alert data to the format required to create new alerts in Oracle Enterprise Manager.

After the `getNewAlerts` operation is complete, the Enterprise Manager Connector Framework performs the `getUpdatedAlerts` operation. Like the `getNewAlerts` operation, it sends a request to the Microsoft SCOM web service for updated alerts. When the response comes back, the `getUpdatedAlerts_response.xsl` file is invoked to transform the Microsoft SCOM alert data to the format required to update the alerts in Oracle Enterprise Manager.

Table A–4 lists the default field mappings between the Microsoft SCOM alert and the Oracle Enterprise Manager alert. These mappings are applicable to new and updated alerts, and must always be the same.

Table A–4 getNewAlerts and getUpdatedAlerts Operation Mappings

Oracle Enterprise Manager alert Attribute	Attribute Type	Req'd?	SCOM Alert Attributes	Value
key1	String	Yes	Set to the Microsoft SCOM alert identifier.	<Identifier>
message	String	Yes	Values from the alert are listed in angle brackets in the Value column.	Name — <Name> Computer Name — <NetbiosComputerName> Severity — <source> Object — <Severity> Rule Id — <MonitoringRuleId>
comment	String	Yes	Values from the alert are listed in angle brackets in the Value column.	Resolution State — <Status> Message — <Description>
producerID	String	No	Value defaulted.	SCOM
targetName	String	Yes	Conditional based on the Microsoft SCOM Principal Name.	Set to <PrincipalName> if the SCOM Principal Name contains data. Set to Unknown if the SCOM Principal Name is blank or missing.
TargetType	String	No	Value defaulted.	scom_managed_host
username	String	No	Value defaulted to no value.	
password	String	No	Value default to no value.	
metricName	String	Yes	Set to the SCOM alert source.	<Source>
category	String	Yes	Set to the SCOM alert source.	<Source>
value	String	Yes	Set to the transaction identifier. This is not part of the alert data. It is provided by the web service for tracking transactions.	<transactionID>
severity	String	Yes	Conditional based on the Microsoft SCOM status and severity.	Set to Clear if the SCOM status is set to 255 (Closed). Set to Informational if the SCOM status is not set to 255 and the SCOM severity is Information. Set to Critical if the SCOM status is not set to 255 and the Microsoft SCOM severity is Error. Set to Warning if the SCOM status is not set to 255 and any other SCOM severity value is specified.

Index

S

T

U

V

W

X