Microsoft®
System Center
Operations Manager 2007

Operations Manager 2007 R2 Connectors Deployment Guide

Microsoft Corporation

Published: April, 2009

Feedback

Send suggestions and comments about this document to momdocs@microsoft.com. Please include the product guide name with your feedback.

Revision History

Release Date	Changes
December, 2008	Original release of this guide.
April, 2009	RC beta release of this guide.

Contents

Operations Manager 2007 R2 Connectors Overview

Operations Manager 2007 R2 Connectors provide Operations Manager 2007 R2 alert forwarding to remote systems, such as an Enterprise Management System (EMS) or a help desk system. After Operations Manager 2007 R2 forwards an alert to a remote system, that alert data is synchronized throughout the lifetime of the alert.

The result of that data synchronization is a robust and seamless systems management environment. Such an environment enables cross-organization support processes to take advantage of the resources and strengths of formerly independent support groups. The ultimate effect is improved enterprise systems health through improved organizational communication.

Sharing data between Operations Manager 2007 R2 and remote systems enables enterprise correlation of events from Windows-based systems, hardware, network, and UNIX systems. Correlating these events allows IT staff to determine the causes of issues and reduce the time to resolution of IT outages.

Synchronization of data between Operations Manager 2007 R2 and remote systems also enables operational groups to use familiar management interfaces. Users update an alert by using their management tool, and the data is updated in tools that are used by other operational groups.

Currently Available Connectors

The following Connectors are currently deployable:

Connector for BMC Remedy ARS

Operations Manager 2007 Connector for the BMC Remedy Action Request System (ARS)

Connector for HP Operations Manager

Operations Manager 2007 R2 Connector for the HP Operations Manager (formerly HP OpenView Operations)

Connector for IBM Tivoli Enterprise Console

Operations Manager 2007 R2 Connector for the IBM Tivoli Enterprise Management Console

Universal Connector

An Operations Manager 2007 R2 Connector that can be installed and configured for potentially any remote system that is hosted on a Windows system or on a supported

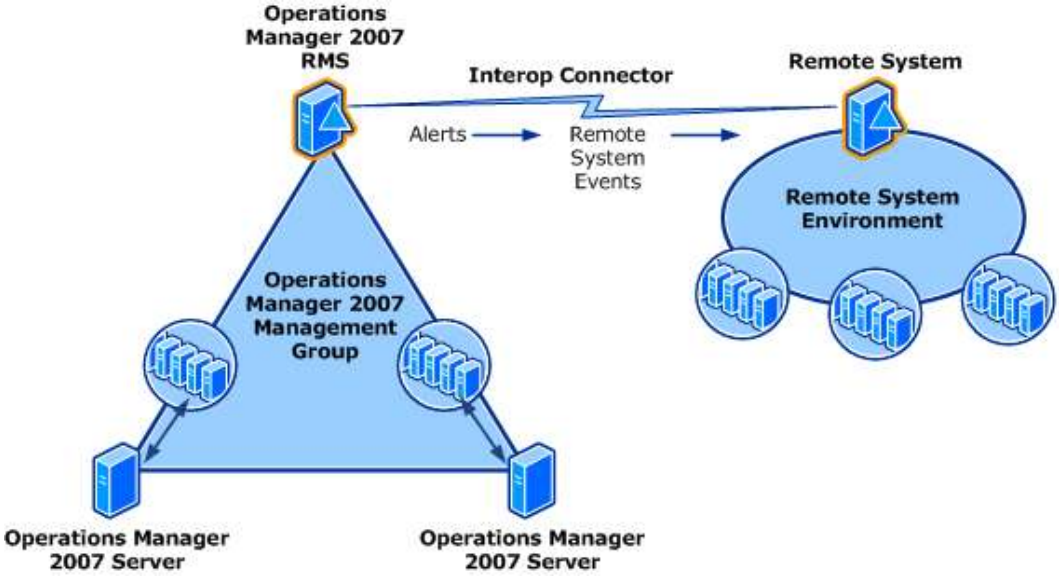
UNIX system.

Features

- Operations Manager 2007 R2 alerts are forwarded to a remote system.
- Operations Manager 2007 R2 alerts are synchronized with remote systems throughout the lifetime of the alert.
- Failover to backup remote system servers is supported.
- The High Availability feature supports failover to secondary Connectors that are installed on other servers in the Operations Manager 2007 R2 domain.
- Multiple Operations Manager 2007 R2 management groups that are communicating with a single remote system are supported.
- Multiple different remote systems can be supported with multiple Connectors that are installed in one Operations Manager 2007 R2 management group.
- Delivery of Operations Manager 2007 R2 alerts is guaranteed by requiring acknowledgement from remote systems.
- The Connector user interface that is integrated into the Operations Manager 2007 R2 console provides the following:
    - Connector health status can be monitored in the Operations Manager 2007 R2 console by using Connector management packs.
    - Connector configuration is limited to Operations Manager 2007 R2 administrators.
    - Operations Manager 2007 R2 servers, remote system servers, and High Availability Connectors can be configured for communications.
    - Alerts forwarding is configured by selecting alert fields, mapping severity, and mapping resolution states to equivalents in a remote system.
    - Selected alerts can be forwarded manually from the Operations Manager 2007 R2 console.
    - Use the Operations Manager 2007 R2 Product Connector Subscription wizard to automatically forward Operations Manager 2007 R2 alerts.
    - Use the Product Connector Subscription wizard to separate alert forwarding for multiple Connectors.

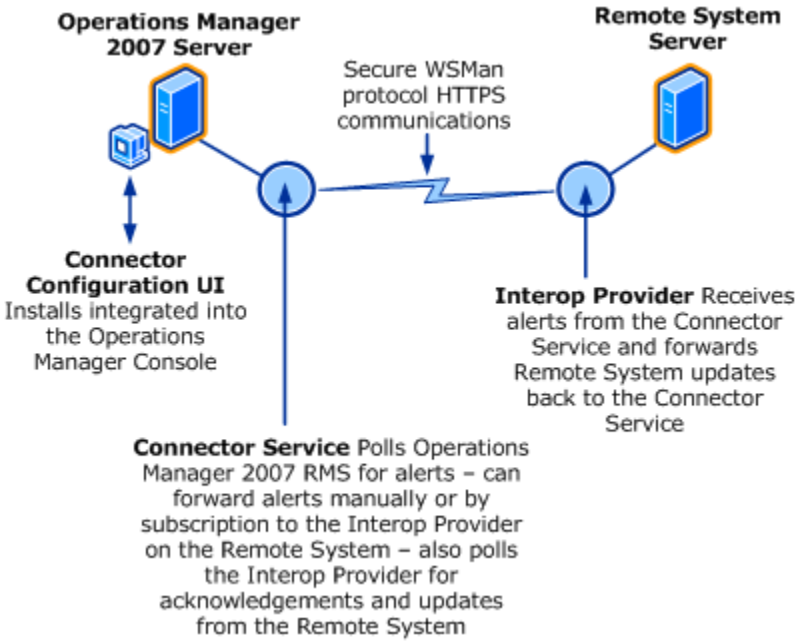
Product Architecture

Operations Manager 2007 Connectors Architecture



Solution Components

Operations Manager 2007 Connectors Components



Each deployed Operations Manager 2007 R2 Connector has the following components:

- **Interop Provider** – This service is installed on a Windows or UNIX server in a supported remote system environment and is automatically started at install. The Interop Provider receives alerts from the Connector Service in the Operations Manager 2007 R2 environment and forwards them to the supported remote system through APIs of that system. The Interop Provider also sends updates on those events back to the Connector Service.
- **Connector Service** – This service is installed on a server in the Operations Manager 2007 R2 environment and is automatically started after configuration is completed. The Connector Service gathers alerts from the Operations Manager 2007 R2 RMS and sends them to the Interop Provider that is installed on a remote system server. The Connector Service also receives updates from that Interop Provider for remote system events that were created from Operations Manager alerts.
- **Connector Configuration UI** – This configuration dialog box is installed on a server on which an Operations Manager 2007 R2 console is installed, and it becomes an integrated component in that console. Use the **Connector Configuration** dialog box to configure communications for Operations Manager 2007 R2 servers with remote system servers. Tabs on the **Connector Configuration** dialog box also provide for mapping Operations Manager alert properties to properties of the remote system's events and for configuring the High Availability feature.

Connectors Predeployment Considerations

This section provides information about what you should consider before you install Operations Manager 2007 R2 Connectors for both the Operations Manager 2007 R2 environment and for supported remote system environments.

System Requirements

The following are system requirements that are necessary to install Operations Manager 2007 R2 Connectors. Requirements are listed for the Interop Provider and the remote system environment, and then for the Operation Manager 2007 environment. The remote system requirements include cases of installation on Windows-based servers and on UNIX-based servers.

Operations Manager 2007 R2 Environment System Requirements

- An Operations Manager 2007 R2 Connector must be installed to operate with Operations Manager 2007 R2. There is no upgrade for systems with previous Microsoft Connectors. Any previous beta Microsoft Connectors must be uninstalled and a new deployment of the wanted Connectors made in an Operations Manager 2007 R2 environment. This includes new Connector Service, Connector Configuration UI, Interop Provider, and Connector Management Pack installations.

- The Connector Service and the Configuration UI components must be installed on computers running Windows Server 2003 SP1 or greater or Windows Server 2008 operating systems.
- Additionally, the Configuration UI component must be installed on a server on which the Operations Manager 2007 R2 Operations console is installed.

  Important

  The Interop Provider Component must be installed before the Connector Service Components.

  Note

  - The Connector Service, the Interop Provider, and the Connector Configuration UI components do not have to be installed on the same server.
  - The Connector Service component does not have to be installed on an Operations Manager 2007 R2 server, but it must be installed on a server in the domain or a trusted domain of the Operations Manager 2007 R2 root management server (RMS).
  - The Connector Configuration UI component does not have to be installed on the Operations Manager 2007 R2 RMS, but it must be installed on a server on which the Operations console is installed.
- An instance of Microsoft SQL Server 2005 must be available within the given Operations Manager 2007 R2 domain.
- .NET Framework version 3.0 SP1 or a later version. For .NET Framework version 3.0 SP1 download, see http://go.microsoft.com/fwlink/?LinkId=120658. .NET Framework 3.0 is only required for the server on which the Connector service is installed; .NET Framework 3.0 is not required for the Connector Configuration UI component if it is installed separately.
- Microsoft Visual C++ 2008 Redistributable Package (x86) if Visual C++ 2008 is not installed. For Visual C++ 2008 Redistributable Package (x86) download, see http://go.microsoft.com/fwlink/?LinkId=117778
- WS-Management 1.1. For WS-Management 1.1 download, see http://go.microsoft.com/fwlink/?LinkId=84599.

Remote Systems on Windows System Requirements

- The Interop Provider component must be installed on a server running Windows Server 2003 or Windows Server 2008.

  Important

  The Interop Provider Component must be installed before the Connector Service Components.

  Important

  The Interop Provider component must be installed on the remote system primary management server for the HP Operations Manager Connector and the IBM Tivoli Enterprise Console Connector.

Important

The Interop Provider component for the HP Operations Manager Connector or the IBM Tivoli Enterprise Console Connector are only validated for installation on the Windows Server 2003 operating system. The Interop Provider component for BMC Remedy ARS Connector and the Universal Connector are validated for both the Windows Server 2003 and the Windows Server 2008 operating systems.

- Microsoft Visual C++ 2008 Redistributable Package (x86) if Visual C++ 2008 is not installed. For Visual C++ 2008 Redistributable Package (x86) download, see http://go.microsoft.com/fwlink/?LinkId=117778
- WS-Management 1.1. For WS-Management 1.1 download, see http://go.microsoft.com/fwlink/?LinkId=84599.

Remote Systems on UNIX System Requirements

The following are UNIX system requirements that apply in all cases of remote systems that are hosted on UNIX systems.

Note

The Interop Provider component must be installed on the remote system primary management server for the HP Operations Manager Connector and the IBM Tivoli Enterprise Console Connector.

The following tables list each specific UNIX system that is supported for each Connector for remote systems on UNIX.

HP Operations Manager Connector
HP-UX 11i v3 (IA64)
HP-UX 11i v3 (PA-RISC)
HP-UX 11i v2 (IA64)
HP-UX 11i v2 (PA-RISC)
Solaris 10 (SPARC)

IBM Tivoli Enterprise Console Connector
IBM AIX 5L 5.3, Technology Level 6, SP5 (PowerPC)
Solaris 10 (SPARC)

Universal Connector
IBM AIX 5L 5.3, Technology Level 6, SP5 (PowerPC)
HP-UX 11i v3 (IA64)
HP-UX 11i v3 (PA-RISC)
HP-UX 11i v2 (IA64)
HP-UX 11i v2 (PA-RISC)
Solaris 10 (SPARC)
Red Hat Enterprise Linux Server release 5.1 (Tikanaga)
SUSE Linux Enterprise Server 10 SP1 (i586)

Installing Connectors

This section provides information about installing all components for Operations Manager 2007 R2 Connector for both the Operations Manager 2007 R2 environment and for supported remote system environments.

In This Section

Installing Connector Components for Remote Systems

Provides instructions for installing Connector components for all supported remote system environments.

Installing Connector Components for Operations Manager 2007 R2

Provides instructions for installing Connector components in the Operations Manager 2007 R2 environment with a Windows Installer or with a command-line silent install.

Installing Connector Components for Remote Systems

This section provides instructions for installing the Operations Manager 2007 R2 Connector component for all supported remote systems. The **Interop Provider** is the only component for

installation in a Windows remote system environment. In a UNIX remote system environment, an additional component called the **Interop Core** is installed along with the **Interop Provider**.

If multiple Connectors were installed in one Operations Manager 2007 R2 environment to connect to various remote systems, an Interop Provider must be installed independently on each remote system.

Important

For installation of the Interop Provider for a remote system in a Windows-based environment, the user account must have local admin privileges for the server on which the Interop Provider is installed. For installation of the Interop Provider for a remote system in a UNIX or Linux environment, the user account must have root privileges for the given remote system.

How to Install the Interop Provider on Windows-based Computers

To install the Interop Provider on Windows-based computers

1. Log on with the privilege level for installing in the given remote system environment, and then access and run the **SciProviderSetup.msi** file to begin the Interop Provider Setup Wizard. On the **Welcome** page, click **Next**.
2. On the **License Agreement** page, read the information carefully, click **I agree**, and then click **Next** to continue.
3. The **Select Provider** page lists the Interop Providers that are supported by the Operations Manager 2007 R2 Connectors. By default, the Interop Universal Provider is selected. Select the Interop Provider that you want to install, and then click **Next**.
4. On the **Custom Setup** page, ensure that the Interop Provider for the Connector you are installing is selected. In all cases the Universal Connector Interop Provider component is also available for installation at the same time. After selections are completed, click **Next**.
5. Click **Next** on the **Ready to install Microsoft Operations Manager 2007 Interop Providers** page to begin installing the Interop Provider. A progress bar is displayed during the installation.
6. Click **Finish** on the **Completed** page to exit the wizard.

   Note

   For Interop Provider installations for the BMC Remedy ARS Connector, a system reboot is required after installation.

Important

If the Interop Provider is installed after the Connector Service is installed and started, the Interop Provider install overwrites the configuration values that are sent by the Connector Service. For example, the **File Format for Provider** value that is set in the **Universal Connector Configuration** dialog box is set to the Interop Provider

installation default value of ".evt". If the Interop Provider is installed after the Connector Service is installed, stop and restart the Connector Service after the Interop Provider installation.

To uninstall the Interop Provider on Windows-based computers

1. From the **Start** menu, click **Control Panel**, and open **Add or Remove Programs**.
2. Select **System Center Operations Manager 2007 Interop Provider**, and then click **Remove**.

How to Install the Interop Provider on UNIX or Linux Systems

Installation of the Interop Provider component for a supported remote system that is deployed on a UNIX platform requires two installation pieces. First, the Interop Core must be installed and then the Interop Provider is installed. There is a unique pair of packages of the Interop Core and Interop Provider for each supported UNIX or Linux platform and supported remote system.

The following are the UNIX and Linux installation packages that are on the Operations Manager 2007 R2 Connector media. Under each supported operating-system processor-architecture combination, the Interop Core package file is listed, followed by the Interop Provider packages that are available for that platform. The Interop Provider packages are identified by the "ovo", "tec", or "unv" designation in the filename.

IBM AIX 5L 5.3, Technology Level 6, SP5 (PowerPC)

scx-*<build-number>*.aix.5.ppc.lpp.gz **(Interop Core package)**

scinterop-*<build-number>*.aix.5.3.ppc-tec.lpp.gz

scinterop-*<build-number>*.aix.5.3.ppc-unv.lpp.gz

HP-UX 11i v2 (IA64)

scx-*<build-number>*.hpux.11iv2.ia64.depot.Z **(Interop Core package)**

scinterop-*<build-number>*.hpux.11iv2.ia64-ovo.depot.Z

scinterop-*<build-number>*.hpux.11iv2.ia64-unv.depot.Z

HP-UX 11i v2 (PA-RISC)

scx-*<build-number>*.hpux.11iv2.parisc.depot.Z **(Interop Core package)**

scinterop-*<build-number>*.hpux.11iv2.parisc-ovo.depot.Z

scinterop-*<build-number>*.hpux.11iv2.parisc-unv.depot.Z

HP-UX 11i v3 (IA64)

scx-*<build-number>*.hpux.11iv3.ia64.depot.Z **(Interop Core package)**

scinterop-*<build-number>*.hpux.11iv3.ia64-ovo.depot.Z

scinterop-<*build-number*>.hpux.11iv3.ia64-unv.depot.Z

HP-UX 11i v3 (PA-RISC)

scx-<*build-number*>.hpux.11iv3.parisc.depot.Z **(Interop Core package)**

scinterop-<*build-number*>.hpux.11iv3.parisc-ovo.depot.Z

scinterop-<*build-number*>.hpux.11iv3.parisc-unv.depot.Z

Solaris 10 (SPARC)

scx-<*build-number*>.solaris.10.sparc.pkg.gz **(Interop Core package)**

scinterop-<*build-number*>.solaris.10.sparc-ovo.pkg.gz

scinterop-<*build-number*>.solaris.10.sparc-tec.pkg.gz

scinterop-<*build-number*>.solaris.10.sparc-unv.pkg.gz

Red Hat Enterprise Linux Server release 5.1 (Tikanaga)

scx-<*build-number*>.rhel.5.x86.rpm **(Interop Core package)**

MSFTscinteropUnv-<*build-number*>.rhel.5.x86.rpm

SUSE Linux Enterprise Server 10 SP1 (i586)

scx-<*build-number*>.sles.10.x86.rpm **(Interop Core package)**

MSFTscinteropUnv-<*build-number*>.suse.10.x86.rpm

After selecting the appropriate package files for installation, copy the files to the /tmp directory on the UNIX platform. After the package files are copied to the /tmp directory, there are two more steps for installation with each package.

1. Uncompress or unzip the package file.
2. Unpack and install files from the package.

The following procedures show the commands for performing these steps on each supported operating system. All samples use the Universal Connector packages for the examples. To install a Connector other than the example provided, replace the string “Unv” with the following case specific identities for the appropriate Connectors:

“Ovo” for HP Operation Manager Connector (formerly HP OpenView Operations)

“Tec” for IBM Tivoli Enterprise Console Connector

The last command in each case is the Interop Provider uninstall command.

IBM AIX 5L 5.3, Technology Level 6, SP5 (PowerPC)

1. To unzip, unpack, and install the Interop Core:

```
gzip -d /tmp/scx-<build-number>.aix.5.pcc.lpp.gz

installp -X -d /tmp/scx-<build-number>.aix.5.ppc.lpp scx.rte
```

2. To unzip, unpack, and install the Interop Provider:

```
gzip -d /tmp/scinterop-<build-number>.aix.5.3.pcc-unv.lpp.gz

installp -X -d /tmp/scinterop-<build-number>.aix.5.3.ppc-unv.lpp
MSFTscinteropUnv.rte
```

3. To uninstall:

```
installp –u MSFTscinteropUnv.rte

installp –u scx.rte
```

HP-UX 11i v3 (IA64)

1. To unzip, unpack, and install the Interop Core:

```
uncompress /tmp/scx-<build-number>.hpux.11iv3.ia64.depot.Z

swinstall -s /tmp/scx-<build-number>.hpux.11iv3.ia64.depot scx
```

2. To unzip, unpack, and install the Interop Provider:

```
uncompress /tmp/scinterop-<build-number>.hpux.11iv3.ia64-unv.depot.Z

swinstall -s /tmp/scinterop-<build-number>.hpux.11iv3.ia64-unv.depot scx
```

3. To uninstall:

```
swremove MSFTscinteropUnv

swremove scx
```

HP-UX 11i v3 (PA-RISC)

1. To unzip, unpack, and install the Interop Core:

```
uncompress /tmp/scx-<build-number>.hpux.11iv3.parisc.depot.Z

swinstall -s /tmp/scx-<build-number>.hpux.11iv3.parisc.depot scx
```

2. To unzip, unpack, and install the Interop Provider:

```
uncompress /tmp/scinterop-<build-number>.hpux.11iv3.parisc-unv.depot.Z

swinstall -s /tmp/scinterop-<build-number>.hpux.11iv3.parisc-unv.depot –x
ask=true MSFTscinteropUnv
```

3. To uninstall:

```
swremove MSFTscinteropUnv

swremove scx
```

Solaris 10 (SPARC)

1. To unzip, unpack, and install the Interop Core:

```
gzip –d /tmp/scx-<build-number>.solaris.10.sparc.pkg.gz

pkgadd -d /tmp/scx-<build-number>.solaris.10.sparc.pkg MSFTscx
```

2. To unzip, unpack, and install the Interop Provider:

```
gzip –d /tmp/scinterop-<build-number>.solaris.10.sparc-unv.pkg.gz

pkgadd -d /tmp/scinterop-<build-number>.solaris.10.sparc-unv.pkg
MSFTscinteropUnv
```

3. To uninstall:

```
pkgrm MSFTscinteropUnv

pkgrm MSFTscx
```

Red Hat Enterprise Linux Server release 5.1 (Tikanaga)

1. To install the Interop Core:

```
rpm -i scx-<build number>.rhel.5.x86.rpm
```

2. To install the Interop Provider:

```
rpm –i MSFTscinteropUnv-<build number>.rhel.5.x86.rpm
```

3. To uninstall:

```
rpm –e MSFTscinteropUnv

rpm –e scx
```

SUSE Linux Enterprise Server 10 SP1 (i586)

1. To install the Interop Core:

```
rpm -i scx-<build number>.sles.10.x86.rpm
```

2. To install the Interop Provider:

```
rpm –i MSFTscinteropUnv-<build number>.suse.10.x86.rpm
```

3. To uninstall:

```
rpm –e MSFTscinteropUnv

rpm –e scx
```

Note

When the Interop Provider installation is complete on UNIX or Linux, the Interop Provider is running.

Installing Connector Components for Operations Manager 2007 R2

This section provides instructions for installing Operations Manager 2007 R2 Connector components in the Operations Manager 2007 R2 environment. When both the **Connector**

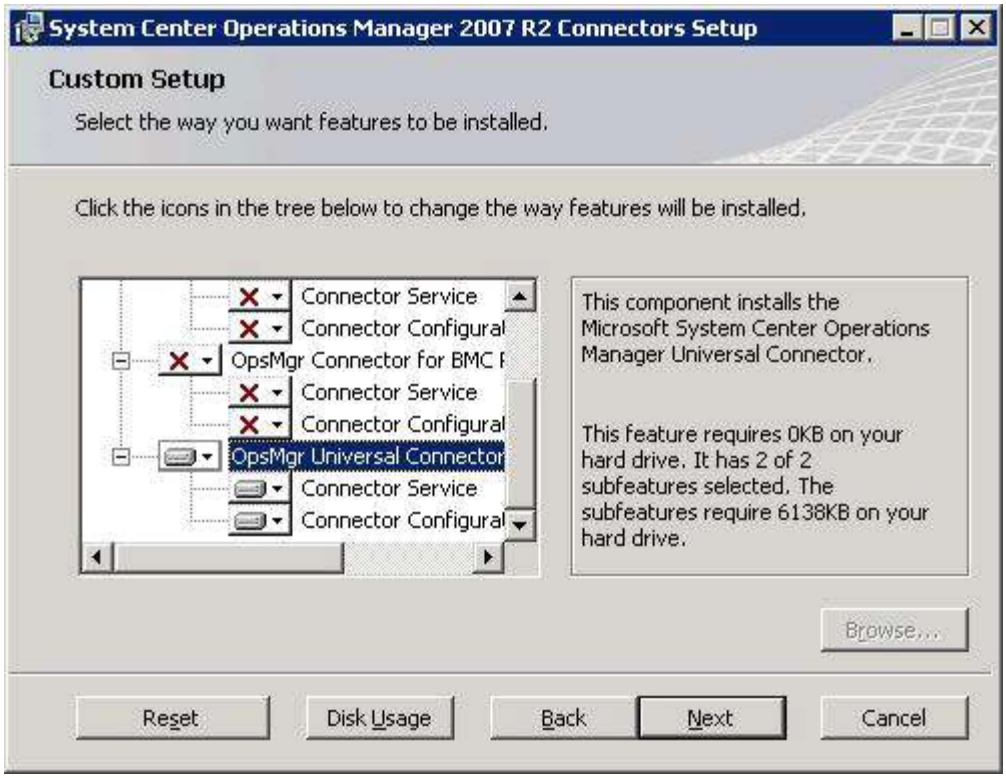
Service and the **Connector Configuration UI** components are installed at the same time, the installation must take place on a server on which an Operations Manager 2007 R2 console is installed. That is because the **Connector Configuration UI** installations are integrated into the Operations Manager 2007 R2 Operations console. If the **Connector Configuration UI** component is installed separately, the **Connector Service** component can be installed on any computer with a supported configuration in the domain or in a trusted domain of the Operations Manager 2007 R2 root management server (RMS).

For information about a command-line silent installation, see the end of the To Install Operations Manager 2007 Connector Components section later in this topic.

Important

The Interop Provider Component must be installed before the Connector Service Components.

The Custom Setup page of the installation wizard.



For the first instance of a Connector service installation on a computer, the **Custom Setup** page appears after the **Welcome** and **End-User License Agreement** pages. By default all components for all Connectors are set to **Entire feature will be unavailable**. Select the Connectors and components you want to install.

The Change, repair, or remove installation page of the installation wizard.

When there is at least one Connector service installed on the computer and you run the installation, the **Change, repair, or remove installation** page appears after the **Welcome** page. The **Remove** button removes all Connectors that are currently installed for the Operations Manager 2007 R2 management group. The **Repair** button is disabled for this release. The **Change** button opens the **Custom Setup** page with all currently installed Connectors set to **Entire feature will be installed on local hard drive**. Leave all installed Connectors that you want to keep set to **Entire feature will be installed on local hard drive**, and also set any other Connector that you want to install to **Entire feature will be installed on local hard drive**.

Important

If you set previously installed Connectors to **Entire feature will be unavailable**, those Connectors are uninstalled.

To install Operations Manager 2007 Connector components

1. Log in as Administrator or with appropriate permissions, access and run the **SciConnectorSetup_x86.msi** file or the **SciConnectorSetup_x64.msi** file to start the Operations Manager 2007 R2 Connector installer.

   Use the SciConnectorSetup_x86.msi file for computers that are 32-bit systems. Use the SciConnectorSetup_x64.msi file for computers that are non-Itanium 64-bit systems.

   Important

A user account with the following permissions is necessary for installing Connectors in the Operations Manager 2007 R2 environment.

- The account must have local admin privileges on the local system and on the local security policies. The account must include granting the logon as a service privilege.
- The account must have Operations Manager 2007 R2 administrator privileges.
- The account must have SQL DBO privileges for all databases involved.
- A domain account with the privileges noted earlier in this topic is necessary when components or functionality are on different systems, such as deployment of High Availability Connectors.

On the **Welcome** page, click **Next**.

2. On the **End User License Agreement** page, read the information carefully, click **I agree**, and then click **Next** to continue.
3. The **Custom Setup** page shows the selection tree for Connectors and their components. By default, all remote system Connectors and all their components are set to **Entire feature will be unavailable**. To enable a Connector, click the down arrow next to the Connector name and select to the Connector that you want to install, and select **Entire feature will be installed on local hard drive**.

   You can set the **Connector Configuration UI** component to **Entire feature will be unavailable** and install it later on a different Operations Manager 2007 R2 server. Make sure that the **Connector Configuration UI** component is installed on a server on which the Operations Manager 2007 R2 console is installed.

   After selecting Connectors to install, the currently selected Connector's installation location appears in the **Installation folder** box. Click **Browse** to make changes.

   Important

   Management Packs for each Connector that is installed are imported into the Operations Manager 2007 R2 RMS when the Connector Configuration wizard runs. The first instance of a Connector deployment imports the Connectors common library management pack, which is a parent management pack for the individual specific remote system management packs. The specific remote system management packs are imported at each Connector deployment. For more information about Connector management packs, see the *Connectors Management Pack Guide for Operations Manager 2007*.

   Important

   You can select more than one remote system Connector to install in the same installation session. For information about configuring alert forwarding subscriptions when more than one remote system Connector is installed in an Operations Manager 2007 R2 management group, see Using the Operations Manager 2007 R2 Product Connector Subscription Wizard.

   Click **Next** after you have set the Connectors and components that you are going to

install.

4. On the **Connector Configuration database** page, provide the following information:
   - **SQL Server Name**: An instance of SQL Server within the domain or within a trusted domain of the Operations Manager 2007 R2 RMS.
   - **SQL Server Database Instance (optional)**: The name of the instance of a database on the designated instance of a SQL Server. This database name can be the same name as the server and is an optional entry
   - **SQL Database Name**: Enter a name for the database that you want to be created for Operations Manager 2007 R2 Connectors. There is only one Connectors database for all Connectors in one Operations Manager 2007 R2 management group. Any instances of additional Connectors that are installed in the same Operations Manager 2007 R2 management group for High Availability functionality also use this same database. If any Connector has already been installed, the Connector SQL database already exists. If you do not change the entry, by default a local SQL database named **SCInterop** is created.
   - **SQL Server Port**: The default entry is 1433.

   Click **Next** to continue.
5. On the **Configure Connector Service Login and High Availability** page, provide the following information:
   - **User name**: By default this shows the account that is running the Windows Installer. This account, which must have Operations Manager 2007 R2 SDK and Config Service permissions for the Operations Manager 2007 R2 management group.
   - **Password**: The password for the above account.
   - **Domain**: By default the domain for the computer on which you are installing the Connector Service is displayed. The computer must be in the domain or in a trusted domain of the Operations Manager 2007 R2 RMS.
   - **High Availability**: Use this check box to designate the installation as a Connector for High Availability installation. For more information about the High Availability feature, see Configuring High Availability

   Click **Next** to continue.
6. The **Ready to install System Center Operations Manager 2007 R2 Connector** page appears if the service log-on information is valid. Click **Next** to continue.
7. The **Installing** page displays installation progress until the installation of all selected components is complete.
8. The **Connector Certificate Retrieval and Installation** page appears if the installation of the Connector service is complete.

   The Connector requires the use of certificates to validate the authenticity of the server on which the Interop Provider is running. The Connector does not work until the certificate has been transferred and correctly imported from the server on which the Interop Provider is running to the server on which Connector is running. During the Interop

Provider installation, a self-signed certificate is generated and stored in the Interop Provider installation directory. The **Connector Certificate Retrieval and Installation** wizard retrieves the certificate and installs automatically it on the server on which the Connector is running. Installing the Connector certificate at installation is optional. However, the Connector certificate must be installed on the server on which the Connector is running before the Connector service is started. If you do not install the Interop Provider certificate, the Connector cannot communicate with the server on which the Interop Provider is running.

Note

The automatic installation process may be insecure. Verify that the certificate thumbprint returned by the wizard is genuine if you choose to proceed with the automatic import process.

Note

The most secure way to transfer the Interop Provider certificate is by manually using physical medium. See **Installing a Connector Certificate with the Command-Line Installation**.

9. By default, automatic installation is selected. Click **Next** to continue.
10. When the Connector certificate is installed, click **OK** to continue.

To configure Operations Manager 2007 Connectors

1. After installation of the Connector service is complete, the **Configure Connectors** page of the Connector Configuration wizard appears. Running the Connector Configuration wizard at installation is optional. However, the Connector Configuration wizard must be run before the Connector service is started. If you do not run the Connector Configuration wizard at installation time, the icon for running the wizard appears on the **Start** menu of the system where the Connector service was installed.

   The **Configure Connectors** page has a button for each supported Connector. To configure a Connector that has been installed, click the button for that Connector. The **Configure Connectors** page returns after each configuration. If multiple Connectors were installed, click each Connector until all installed Connectors are configured.

   When all Connectors are completed, or to skip configuring Connectors, click **Done**.
2. When the **OpsMgr Connector for <EMS> Connector Configuration** dialog box appears. provide the following information.

   For the **Server names** section:

   - **Operations Manager server name**: The name of the Operations Manager 2007 R2 management group RMS.
   - **<EMS> server name**: The name of the remote system server on which the Interop Provider component will be installed.

   For the **Web Services for Management (WS-Man) server credentials** section:

- **User name**: A user from the remote system server with adequate permissions for Web Services for Management (WS-Man). For Windows, the user must be the local administrator for the remote system environment. For UNIX, the user can be any account with appropriate permissions for the remote system environment.
- **Password**: The password for the user.

For configuration of the BMC Remedy ARS Connector, this dialog box also contains a **Remedy server credentials** section. In this section, provide the following information:

- **Server version**: Select V71 or V63 from the Server version list according to the ARS version being used.
- **User name**: This is the Remedy user as specified in Appendix A - The BMC Remedy ARS Connector as **opsmgr**.
- **Password**: The password for the user.
- **Authentication**: If a credentials authentication system is enabled for Remedy ARS, enter the appropriate string for authentication. If an authentication system is not implemented, leave this field blank.
- **Host name**: The server name for the computer on which the BMC Remedy ARS is installed.

Click **Configure** to continue.

3. Click **Finish** on the **Completed** page to exit the setup wizard.

To uninstall the Connector

1. When any Operations Manager 2007 R2 Connectors have been installed on a computer, log on as Administrator to uninstall the Connector. Use the Windows **Add or Remove Programs** function, or use the Connector installation files, **SciConnectorSetup_x86.msi** or **SciConnectorSetup_x64.msi**, to start the Operations Manager 2007 R2 Connectors installation wizard.
2. When one or more Connectors is installed, the installation wizard displays the **Change, repair, or remove installation** page.

   Click **Remove** to begin removing all installed Connectors.

   Click **Change** to remove specific components or specific Connectors.

Installing a Connector with the Command-Line Silent Installation

Use the command-line properties to execute the Connector setup .msi file with the Microsoft Windows Installer. This enables unmonitored and scripted installations. The following code example is the syntax for the silent installation command.

Important

Microsoft Windows Installer public properties must be uppercase, such as *PROPERTY=value*. For more information about Windows Installer, see http://go.microsoft.com/fwlink/?LinkId=137320.

`msiexec /i <.msi-filename> /qn /l*v connectorinstall.log <REQUIRED-PROPERTIES><REMEDY-PROPERTIES><OPTIONAL-PROPERTIES>`

<.msi-filename>

`SciConnectorSetup_x86.msi` or `SciConnectorSetup_x64.msi`

<REQUIRED-PROPERTIES>

`SERVICE_USER="`*<user-name>*" - account used to set up the Connector service.

`SERVICE_DOMAIN="`*<domain>*" – the domain for the computer on which you are installing the Connector service.

`SERVICE_PASSWORD="`*<password>*" – password for the account used to set up the Connector service.

`SQLSERVER="`*<SQL-server-name>*" – name of the instance of SQL Server that will hold the Connector database.

`OPSMGRSERVER="`*<OpsMgr-server-name>*" – name of the Operations Manager 2007 R2 RMS.

`PROVIDERSERVER="`*<Provider-server-name>*" – name of the remote provider server.

`WSMANUSERNAME="`*<WS-Man-user-name>*" – account from the remote system to be used for communications.

`WSMANUSERPASSWORD="`*<WS-Man-password>*" – password for the remote system communications account.

`ADDLOCAL="`*<Connector>,<ConnectorService>,<ConnectorUI>*" – one of the following sets of four properties that identify which Connector to install.

```
OVO,OVOService,OVOUI

TEC,TECService,TECUI

Universal,UniversalService,UniversalUI

Remedy,RemedyService,RemedyUI
```

<REMEDY-PROPERTIES>

`REMEDYVERSION="`*<Remedy-server-version>*" – enumerated type specifying the Remedy ARS server version being used. Accepted values are V63 or V71.

`REMEDYUSERNAME="`*<Remedy-user-name>*" – Remedy ARS remote system communications account as specified in the Operations Manager 2007 R2 console.

`REMEDYPASSWORD="`*<Remedy-password>*" - password for the Remedy ARS remote

system communications account.

REMEDYAUTH="*<string>*" - if a credentials authentication system has been enabled on the Remedy ARS server, enter the appropriate authentication string. If an authentication system has not been implemented, you may omit this property.

REMEDYSERVER="*<Remedy-server-name>*" – the server name for the computer on which Remedy ARS is installed.

<OPTIONAL-PROPERTIES>

SQLINSTANCE="*<database-instance>*" – name of the instance of the database to use. The default instance is used by default.

DBNAME="*<database-name>*" – name to use for the Connector database. If not specified, SCInterop is used.

EMSPORT="*<port-value* >" – For TEC connector only, sets the server listening port. The default value is "0", which designates using the Port Mapper on UNIX platforms. A TEC administrator can provide a port value for TEC on a Windows operating system, which is typically "5529".

SERVICE_HA="1" – this property must be set when you are installing a High Availability Connector.

The following is an example of a silent installation command for a Remedy ARS server on an x86 Windows-based system.

```
msiexec /qn /i SciConnectorSetup_x86.msi /l*v connector.log
ADDLOCAL="Remedy,RemedyService,RemedyUI" SERVICE_USER="user-name" SERVICE_DOMAIN="domain"
SERVICE_PASSWORD="password" SQLSERVER="SQL-server-name" OPSMGRSERVER="OpsMgr-server-name"
PROVIDERSERVER="Provider-server-name" EMSPORT="port-value" WSMANUSERNAME="WS-Man-user-
name" WSMANUSERPASSWORD="WS-Man-password" REMEDYVERSION="Remedy-version"
REMEDYUSERNAME="Remedy-user-name" REMEDYPASSWORD="Remedy-password" REMEDYAUTH="string"
REMEDYSERVER="Remedy-server-name"
```

If Authorization is not configured on your Remedy ARS server, do not include the REMEDYAUTH parameter.

The following is an example of a silent installation command for a High Availability Universal Connector on an x86 Windows-based system.

```
msiexec /i SciConnectorSetup_x86.msi /qn /l*v connectorinstall.log SERVICE_USER="user-
name" SERVICE_DOMAIN="domain" SERVICE_PASSWORD="<password>" SQLSERVER="<SQL-server-name>"
OPSMGRSERVER="<OpsMgr-server-name>" PROVIDERSERVER="<Provider-server-name>"
WSMANUSERNAME="<WS-Man-user-name>" WSMANUSERPASSWORD="<WS-Man-password>"
ADDLOCAL="Universal,UniversalService,UniversalUI" SERVICE_HA="1"
```

Installing a Certificate with the Command-Line Installation

Use the command-line application, Scicert.exe, to install the Interop Provider certificate on the Connector server. Installing the Interop Provider certificate enables secure communication between the server on which the Interop Provider is running and the server on which the Connector is running. The file, Scicert.exe, is stored in the Operations Manager 2007 R2 Connector installation directory. The following code example is the syntax for the certificate installation command.

```
scicert <REQUIRED-PROPERTIES><OPTIONAL-PROPERTIES>
```

<REQUIRED-PROPERTIES>

`HOST=`"*<certificate-host>*" – the location where the Interop Provider certificate is installed.

`USER=`"*<user-name>*" – the account used to set up the Connector service.

`PASSWORD=`"*<password>*" – password for the account used to set up the Connector service.

<OPTIONAL-PROPERTIES>

`SILENT`"*<silent>*" – enumerated type specifying whether the results should be displayed. Accepted values are “0” and “1”, “1” is default.

Installing for High Availability

The High Availability feature of the Operations Manager 2007 R2 Connector enables failover to secondary Connectors without loss of data. High Availability supports server or communications failure among servers that are configured for High Availability. Data from higher-level failure, such as Operations Manager 2007 R2 root management server (RMS) or total management group failure cannot be recovered with the High Availability feature.

High Availability is enabled by installing the Connector on each server to be configured for High Availability. There is a **High Availability** check box on the **Configure Connector Service Login and High Availability** page of the Connector installation wizard that designates an installation as a High Availability installation.

After installation of all Connectors in a High Availability group, use the **High Availability** tab of the **Connectors Configuration** dialog box to configure the failover communications order for those Connectors. For more information about using the **High Availability** tab of the **Connectors Configuration** dialog box, see Configuring High Availability.

Important

When you install Connectors for High Availability functionality, ensure that the following points are followed.

High Availability is selected on the **Configure Connector Service Login and High Availability** installation wizard page for all Connector service installations for a High Availability group.

You are using the same SQL Connectors database and database server for all Connector installations for the High Availability group.

The **Connector Service** installation is required for all High Availability installations, but the **Configuration UI** component is optional. There must be at least one installation of the **Configuration UI** component within an Operations Manager 2007 R2 management group.

When secondary installations are done for High Availability Connectors, the configuration for that Connector in that Operations Manager 2007 R2 management group is overwritten at each separate installation. Thus only the configuration as set by the last installation applies. Do not customize the Connector configuration with the **Connectors Configuration** dialog box from the **Administration** pane of the Operations Manager 2007 R2 Operations console until all secondary Connectors are installed.

Important

If the Interop Provider is installed after the Connector Service is installed and started, the Interop Provider installation overwrites the configuration values that are sent by the Connector Service. For example, the **File Format for Provider** value set in the **Universal Connector Configuration** dialog box is set to the Interop Provider installation default value of ".evt". If the Interop Provider is installed after the Connector Service is installed, stop and restart the Connector Service after the Interop Provider installation.

Configuring Connectors

This section provides information about configuring an Operations Manager 2007 R2 Connector after it has been installed in an Operations Manager 2007 R2 environment. During Connector installation, the **Configure Connectors** page of the installation wizard enables default Connector configuration. The **Connectors Configuration** dialog box enables custom configuration for a Connector.

Important

The Appendices provide information specific to the Operations Manager 2007 R2 Connector for each supported remote system. This can include information about additional configuration steps that must be taken in the specific remote system or information about remote system configuration that is done during the Connector components installation.

Using the Connector Configuration Dialog Box

Use the **Connector Configuration** dialog box that is specific to each installed Connector to configure communications and the mapping of alert to remote system event information. This dialog box is available from the Operations Manager 2007 R2 console and has the following tabs.

Note

The Universal Connector, which is generic, does not have the **Severity Mapping** tab or the **Resolution State Mapping** tab on its **Universal Connector Configuration** dialog box. The tabs on the **Universal Connector Configuration** dialog box are the same as the other **Connector Configuration** dialog boxes in all other respects. However, the HP Operations Manager **Connector Configuration** dialog box, has a **Property Mapping** tab instead of an **Alert Fields** tab.

<EMS> server

You can use this tab to configure the remote system servers for communications with the Connector. For information about using the **<EMS> server** tab, see Configuring Servers for Communications.

Operations Manager

You can use this tab to configure Operations Manager 2007 R2 servers for communications with the Connector. For information about using the **Operations Manager** tab, see Configuring Servers for Communications.

Alert Fields or Property Mapping (HP Operations Manager only)

You can use this tab to select additional Operations Manager alert fields that are forwarded with alerts to the remote system. For HP Operations Manager, this tab is replaced with the **Property Mapping** tab that is used to map Operations Manager 2007 R2 alert properties to HP Operations Manager event properties. For information about using this tab, see Configuring Operations Manager 2007 R2 Alerts for Forwarding.

Severity Mapping

You can use this tab to map Operations Manager severity levels to the remote system equivalents. For information about using the **Severity Mapping** tab, see Configuring Operations Manager 2007 R2 Alerts for Forwarding.

Resolution State Mapping

You can use this tab to map Operations Manager resolution states to the remote system equivalents. For information about using the **Resolution State Mapping** tab, see Configuring Operations Manager 2007 R2 Alerts for Forwarding.

High Availability

You can use this tab to configure the local Connector for High Availability functionality. Each server that is to have a High Availability Connector must have independent

Connector installation. For information about using the **High Availability** tab, see Configuring High Availability.

To open the Connector Configuration dialog box

1. In the **Administration** navigation pane of the Operations Manager 2007 R2 console find the **Product Connectors** node. Under the **Product Connectors** node is the **Interop Connectors** object. Under **Interop Connectors**, click the Connector that you want to configure.
2. In the **Results** pane, right-click the Connector to be configured, and then click **Properties** to display the **Connector Configuration** dialog box for that Connector.

Configuring Servers for Communications

You can use the **<EMS> Connector Configuration** dialog box to configure Operations Manager 2007 R2 and remote system servers for communications with the Connector. The **<EMS> Connector Configuration** dialog box has the following tabs for configuring Connector environment servers.

- **<EMS> Server** (where <EMS> is a placeholder for the specific remote system name)
- **Operations Manager**

<EMS> Server Configuration

You can use the **<EMS> Server** tab of the **Connector Configuration** dialog box to configure remote system servers for communications with the Connector.

The **<EMS> Server** tab has the following sections and elements.

Enterprise Management System (EMS) Server Communication Order

Move Up

Moves the selected server name up in the list.

Move Down

Moves the selected server name down in the list.

Remove Selected Server

Removes the selected server name from the list.

Add Server to List

Adds to the list a remote system server that has an Interop Provider installed. Polling and other Connector communications are first attempted with the top server on the list. The communication attempts continue down the list and loop through the list according to the server settings in the lower section of the tab. Server names must be derived from other sources.

Caution

Each remote system server in this list must have an Interop Provider installed or communications attempts will fail.

Caution

Do not use the name **localhost**; spell out the host name.

Settings in the following sections of the tab apply or appear for the selected server.

Web Services for Management (WS-Man) Server Credentials

User name

For Windows operating systems, the user must be the local administrator the for the remote system environment on the server that is being added. For UNIX or Linux, the account can be any user with appropriate permissions for the remote system environment.

Password

Enter the password for the designated user for Web services on the remote system server that is being added.

WS-Man port

TCP port 1270 is set by default and cannot be changed.

The following are the sections of the **<EMS> Server** tab that have unique sets of elements for each Connector.

OVO Server

Server polling interval (in seconds)

Set a value, in seconds, to determine the time between Interop Provider polling of the remote system server for acknowledgements or updated events. **Default=30**

Receive updates from Operations Manager

Select this check box to enable the forwarding of updated Operations Manager 2007 R2 alerts to HP Operations Manager.

Send updates to Operations Manager

Select this check box to enable the forwarding of updated remote system events to Operations Manager 2007 R2.

Convert host name to IP address

Select this check box to automatically convert the host name entered in the list to an IP address.

TEC Server Settings

Server polling interval (in seconds)

Set a value, in seconds, to determine the time between Interop Provider polling of the remote system server for acknowledgements or updated events. **Default=30**

Server listening port

Set to 0 for to use the Port Mapper for TEC on a UNIX platform. Otherwise set as noted by the TEC administrator, typically 5529 for TEC on Windows operating systems. **Default=0**

Receive updates from Operations Manager

Select this check box to enable the forwarding of updated Operations Manager 2007 R2 alerts to IBM Tivoli Console.

Send updates to Operations Manager

Select this check box to enable the forwarding of updated remote system events to Operations Manager 2007 R2.

EMS Server with the Universal Connector

Server polling interval (in seconds)

Set a value, in seconds, to determine the time between Interop Provider polling of the remote system server for acknowledgements or updated events. **Default=30**

File format for Provider

Select the drop down value of XML for forwarding alerts as XML files. Select EVT for forwarding alerts as text properties files. **Default=XML**

Note

Alerts forwarded to the Interop Provider on Windows remote systems are validated for XML format, alerts forwarded to the Interop Provider on UNIX remote systems are validated for EVT text format. For more information about Universal Connector alert messaging formats, see Using the Universal Connector.

Receive updates from Operations Manager

Select this check box to enable the forwarding of updated Operations Manager 2007 R2 alerts to the active remote system.

Send updates to Operations Manager

Select this check box to enable the forwarding of updated remote system events to Operations Manager 2007 R2.

Operations Manager Server Configuration

You can use the **Operations Manager** tab of the **Connector Configuration** dialog box to configure the Operations Manager 2007 R2 root management server (RMS) that communicates with the Connector. Because one Operations Manager 2007 R2 management group can have only one RMS, there can be no other Connector RMS to add to the list. Use this list to reconfigure communications when an Operations Manager 2007 R2 management group has been reconfigured with a new RMS.

Caution

Listing an Operations Manager 2007 R2 RMS of a different management group causes forwarding of alerts from a different Operations Manager 2007 R2 database.

The **Operations Manager** tab has the following sections and elements.

Operations Manager Server Communication Order

Move Up

Moves the selected server name up in the list.

Move Down

Moves the selected server name down in the list.

Remove Selected Server

Removes the selected server name from the list.

Add Server to List

Adds an Operations Manager 2007 R2 server that communicates with the Connector. Polling and other Connector communications are first attempted with the top server on the list. The communication attempts continue down the list and loop through the list according to the server settings in the lower section of this **Operations Manager** tab. Server names must be derived from other sources.

Caution

Do not use the name **localhost**; spell out the host name or use an IP address. Only Operations Manager 2007 R2 root management servers (RMSs) can communicate with servers of remote systems.

Settings in the following section of the tab apply or appear for the selected server.

Operations Manager Server Settings

Server polling interval (in seconds)

Set the number of seconds between polling for new and updated Operations Manager 2007 R2 alerts. **Default=30**

Forward historical alerts (number of hours old)

Set the number of hours to go back and look for alerts to be sent to the remote system. **Default = 0** (indicating that no historical alerts are sent upon starting or restarting the Connector service)

Caution

If the Connector service is turned off and turned back on while the Forward Historical alerts setting is 0, all alerts that occur when the service is inactive will not be forwarded to the remote system.

Maximum field size

Set the maximum number of characters that can be sent as data for each field. **Default=2000**

Maximum number of delivery attempts

Set the number of attempts to send Operations Manager 2007 R2 alerts if transmission fails. **Default=5** (Set to 0 for infinite.)

Number of polls to wait for response

Set the number of polls to hold an alert in cache. Multiply the **Server polling interval** by the **Number of polls to wait** for total cache holding period. For example, default settings hold an alert in cache for five minutes. **Default=10**

Send updates for closed alerts only

Select this check box to forward alert updates to the remote system server only when Operations Manager 2007 R2 alert status is set to **closed**.

Configuring Operations Manager 2007 R2 Alerts for Forwarding

You can use the **<EMS> Connector Configuration** dialog box to map properties of Operations Manager 2007 R2 alerts to synchronize with events in other remote systems. The **<EMS> Connector Configuration** dialog box has the following tabs for configuring alerts for forwarding.

- **Alert Fields**

  IBM Tivoli Enterprise Console Connector

  BMC Remedy ARS Connector

  Universal Connector
- **Property Mapping**

  HP Operations Manager
- **Severity Mapping**

  HP Operations Manager

  IBM Tivoli Enterprise Console Connector

  BMC Remedy ARS Connector
- **Resolution State Mapping**

  HP Operations Manager

  IBM Tivoli Enterprise Console Connector

  BMC Remedy ARS Connector

Setting Alert Fields for Forwarding with Alerts

You can use the **Alert Fields** tab of the **<EMS> Connector Configuration** dialog box to select Operations Manager 2007 R2 alert fields to be included with the alert that is sent to the remote system.

The **Alert Fields** tab has the following sections with check boxes for alert fields grouped by function.

Alert

- **Category**
- **Context**
- **Description**— default
- **Modified By**— default
- **Modification Time**— default

Custom fields

- **Custom Field 1**— default
- **Custom Field 2**— default
- **Custom Field 3**— default
- **Custom Field 4**— default
- **Custom Field 5**— default
- **Custom Field 6**
- **Custom Field 7**
- **Custom Field 8**
- **Custom Field 9**
- **Custom Field 106**

Connector

- **Connector Status**
- **Connector ID**

Monitoring objects

- **Monitoring Object Display Name**
- **Monitoring Object Full Name**
- **Monitoring Object ID**
- **Monitoring Object in Maintenance Mode**— default
- **Monitoring Object Health State**— default

Monitoring Object Name— default

Monitoring Object Path— default

Management Server Name— default

Misc

Computer Name— default

Domain Name— default

Last Modified By nonConnector

Maintenance Mode Last Modified

Monitoring Class ID

Monitoring Rule ID

Principal Name

Resolve By

Owner

Site Name

State Last Modified

Time Added

Time Resolution State Modified

Time Resolved

Company Knowledge

Mapping Properties from Operations Manager 2007 Alerts to HP Operations Manager Events

You can use the **Property Mapping** tab of the **HP Operations Manager Connector Configuration** dialog box to map Operations Manager 2007 R2 alert properties to HP Operations Manager event properties.

The **Property Mapping** tab has the following sections and elements.

Current OVO to Operations Manager Property Mappings

OVO event property

This column displays the configured HP Operations Manager event properties.

Operations Manager alert property

This column displays the configured Operations Manager 2007 R2 alerts as mapped to the HP Operations Manager event properties.

Remove Mapping

Click this button to remove a selected set from the mappings table.

Map OVO Event Property to Operations Manager Alert Property

OVO event property

Select from this list of HP Operations Manager event properties.

Operations Manager alert property

Select from this list of Operations Manager 2007 R2 alert properties to map to the selected HP Operations Manager event property.

Add Mapping

Click this button to add the currently selected mapping to the mappings table.

Optional Text Messages

OVO event properties

This column displays the configured HP Operations Manager event properties.

Optional text message

Use this column to enter and map optional text messages associated to HP Operations Manager event properties.

Mapping Operations Manager 2007 Severity Levels to the Remote System

The **Severity Mapping** tab of the **<EMS> Connector Configuration** dialog box enables you to map Operations Manager 2007 R2 severity levels to equivalent remote system settings.

The **Severity Mapping** tab has the following sections and elements.

Current <EMS> to Operations Manager Severity Mappings

<EMS> severity

This column displays the configured remote system severity.

Operations Manager severity

This column displays the configured Operations Manager 2007 R2 severity as mapped to the remote system severity.

Remove Mapping

Click this button to remove a selected set from the mappings table.

Map <EMS> Severity to Operations Manager Severity

<EMS> severity

Select from this list of the remote system severity levels.

Operations Manager severity

Select from this list of Operations Manager 2007 R2 severity levels to map to the selected remote system severity level.

Add Mapping

Click this button to add the currently selected mapping to the mappings table.

Mapping Operations Manager 2007 Resolution States to the Remote System

The **Resolution State Mapping** tab of the **<EMS> Connector Configuration** dialog box enables you to map Operations Manager 2007 R2 resolution states to equivalent remote system settings.

The **Resolution State Mapping** tab has the following sections and elements.

Current <EMS> to Operations Manager Resolution State Mappings

<EMS> resolution state

This column displays the configured remote system resolution state.

Operations Manager resolution state

This column displays the configured Operations Manager 2007 R2 resolution state as mapped to the remote system resolution state.

Remove Mapping

Click this button to remove a selected set from the mappings table.

Map <EMS> Resolution State to Operations Manager Resolution State

<EMS> resolution state

Select from this list of remote system resolution state values.

Operations Manager resolution state

Select from this list of Operations Manager 2007 R2 resolution states to map to the selected remote system resolution state value.

Add Mapping

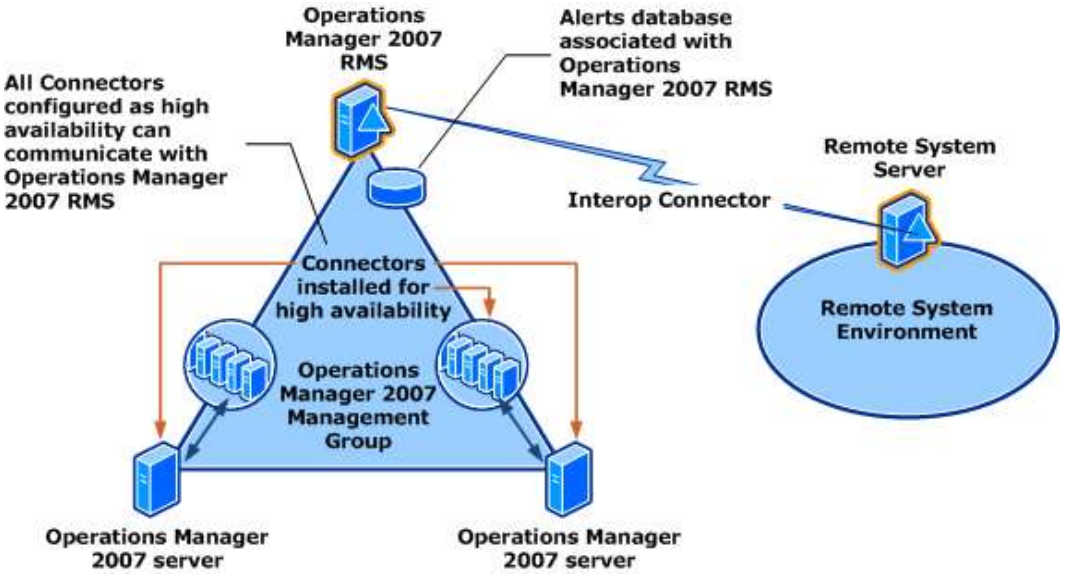
Click this button to add the currently selected mapping to the mappings table.

Configuring High Availability

You can use the **<EMS> Connector Configuration** dialog box to configure High Availability Operations Manager 2007 R2 Connectors or to monitor their availability.

For High Availability configuration, you must install Connectors on multiple servers. Each High Availability Connector is installed with the High Availability feature enabled on the **Configure Connector Service Login and High Availability** page of the Connector installation. All High Availability Connector installations must use the same SQL database and must be installed within the environment of one Operations Manager 2007 R2 management group.

Considerations of High Availability failover of servers in the High Availability server communication order table.



Using High Availability

You can use the **High Availability** tab of the **<EMS> Connector Configuration** dialog box to configure Operations Manager 2007 R2 servers for High Availability communications for the Connector service.

The **High Availability** tab has the following sections and elements.

High Availability Configuration

High Availability polling interval (in seconds)

Use this box to enter a value in seconds. This value is the interval for polling for the availability status of the servers configured with High Availability. **Default=30**

High Availability tolerance

Use this box to enter a value for the number of High Availability polling intervals during which a High Availability server can fail to respond before it is designated offline. For example, default settings designate a High Availability server as offline if there is no response to the polling signal in a 90-second period. **Default=3**

High Availability Server Communication Order

Host name (Server)

First column in the server list table; displays the server name. All servers in the

Operations Manager 2007 R2 management group that have Connectors installed for the given remote system appear in the list.

State

Second column in the server list table; displays the availability state as of last polling. Possible states are:

Active – Connector currently in use.

Passive – Connector available but not currently in use.

Offline – Connector currently unavailable.

Last heartbeat

Third column in the Server list table; displays the timestamp of the last successful polling.

Move Up

When there are multiple servers listed in the server list table, click this button to move the selected server up one space.

Move Down

When there are multiple servers listed in the server list table, click this button to move the selected server down one space.

Refresh List

Click this button to refresh all information in the server list table to the latest polling.

Using the Universal Connector

The Universal Connector is designed to deliver an Operations Manager 2007 R2 alert through the Connector service to any remote system that is deployable on Windows operating systems or supported UNIX and Linux platforms. This section provides the necessary communication information and sample alert formats to enable a remote system administrator or developer to enable Operations Manager 2007 R2 alert forwarding with the Universal Connector.

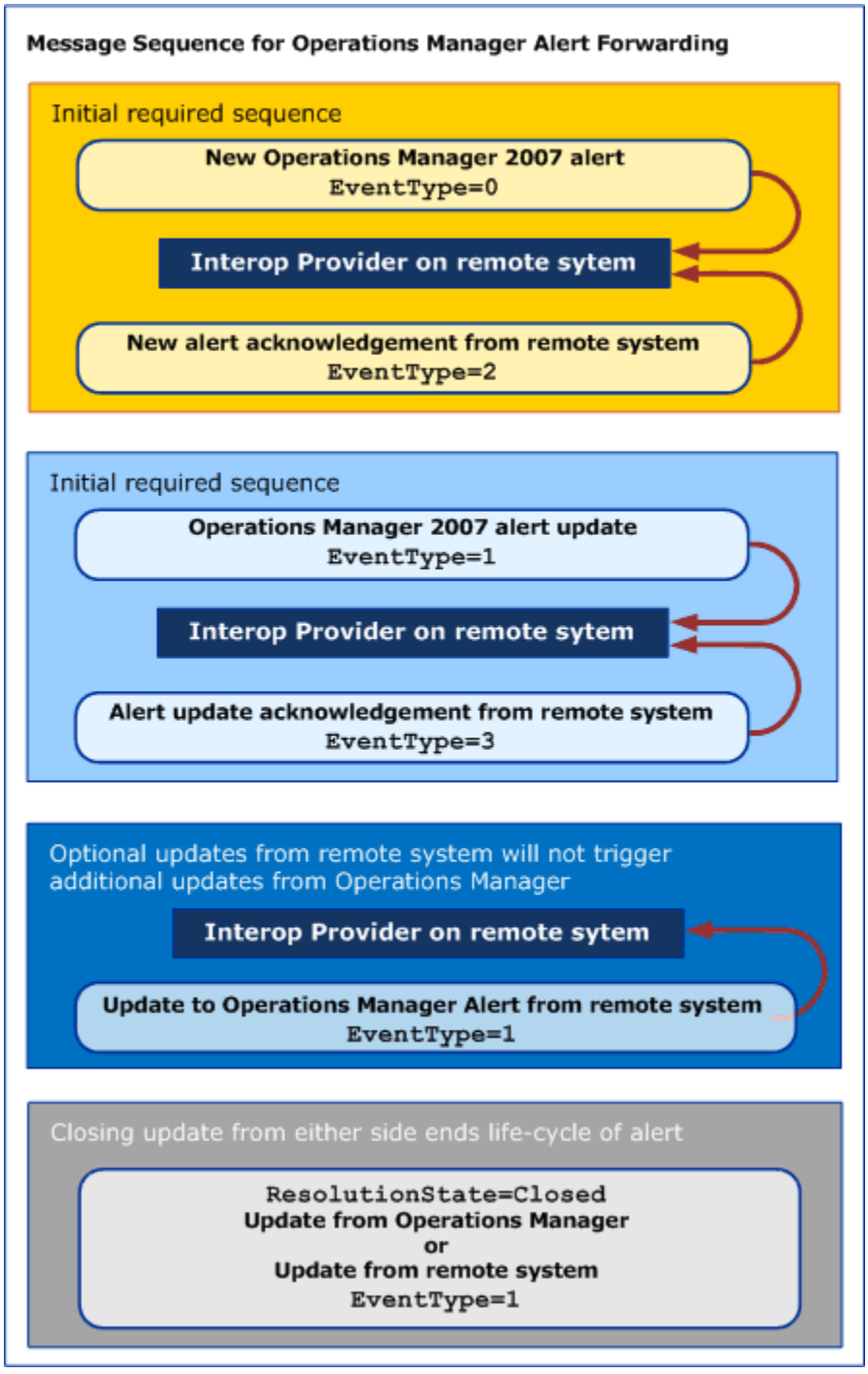
Alert Communication Life Cycle and Requirements

When the Universal Connector has been installed and configured, the service is running and can forward Operations Manager 2007 R2 alerts to the remote system by using the configuration that is described in Configuring Connectors. Operations Manager 2007 R2 alerts are forwarded manually or with a Product Connector Subscription that is described in Controlling Connector Forwarding.

A remote system administrator or developer must implement integration logic to transfer the data to the remote system from the Operations Manager 2007 R2 alert and alert update files that the Interop Provider saves on the remote system server. This process can also include providing files to the Interop Provider from the remote system as acknowledgements to the alerts and alert updates from Operations Manager 2007 R2. The process should also provide files to the Interop Provider from the remote system for updates that the remote system posts against the events that came from Operations Manager 2007 R2 alerts. This transfer process also includes translating or mapping the field or property names and values that are known on the remote system to those that are used by Operations Manager 2007 R2. The **EventType** field is required in all messages and determines whether the message is a new alert, new alert acknowledgement, alert update, alert update acknowledgement, or remote system update.

See Appendix D - The Universal Connector for PowerShell samples for the needed integration logic.

The following diagram shows the necessary and optional communication sequences that take place for forwarding Operations Manager 2007 alerts to a remote system by using the Universal Connector.



Alerts and alert updates are forwarded from Operations Manager 2007 R2 to the remote system contain fields that are designated on the **Alert Fields** tab of the **Universal Connector**

Configuration dialog box. The following table shows the required fields contained in alerts and updates that are forwarded from Operations Manager 2007 R2. If all the selectable fields in the **Alert Fields** tab are cleared, this table shows the fields that are still reported in the alerts and alert updates. Additionally, the table shows the fields that must be returned to Operations Manager 2007 R2 in the acknowledgements and updates from the remote system.

Minimum or Required Alert, Update, and Acknowledgement Fields

Message Type	Minimal or Required Fields

New Operations Manager alert	`AlertID`
	`EventType=0`
	`ManagementGroupName`
	`Priority`
	`ResolutionState`
	`Status`

Update from Operations Manager alert	`AlertID`
	`EventType=1`
	`ManagementGroupName`
	`Priority`
	`ResolutionState`
	`Status`

Remote System acknowledgement of new alert	`AlertID`
	`EventID`
	`EventType=2`
	`ManagementGroupName`

Remote System acknowledgement of alert update	`AlertID`
	`EventID`
	`EventType=3`
	`ManagementGroupName`

Remote System update of Operations Manager alert	`AlertID`
	`EventType=1`
	`ManagementGroupName`

The only field in acknowledgement messages from the remote system that writes to the Operations Manager 2007 R2 database is the `EventID` field. The value from that field writes to the `TicketID` field for that alert.

The following message fields of updates from remote systems can write to the Operations Manager 2007 R2 database.

```
CustomField1-10

EventID

OwnerName

ResolutionState
```

The following are the folders or directories relative to the Interop Provider installation folder where Universal Connector messages are delivered to and returned from. These paths are the same for Windows operating systems or UNIX platforms. The remote-system returning file name must be <*filename*>.`xml` for Windows operating systems or <*filename*>.`evt` for UNIX and Linux platforms.

Path for messages the Interop Provider receives from Operations Manager 2007 Universal Connector:

%ProviderInstallDirectory%\UnvEvents\FromOpsMgr

Path for messages the Interop Provider receives from the remote system:

%ProviderInstallDirectory%\UnvEvents*%ManagementGroup%*

Alert Message Formats

The following are samples of a simple alert message that is forwarded from the Connector service to the Interop Provider on a remote system. The alert must be sent in XML format (*.xml) for Windows operating systems and as properties in a text file (*.evt) for UNIX and Linux platforms. For each type of platform, acknowledgement or update messages are expected to be returned to Operations Manager 2007 R2 from the Interop Provider in the same format as forwarded to the Interop provider.

Note

The alert message format is configurable in the **Universal Connector Configuration** dialog box as XML or EVT. XML is the default for Windows operating systems and EVT is the default for UNIX platforms.

XML Format

The following is a sample Operations Manager 2007 R2 alert that is forwarded to a remote system on a Windows operating system in XML format.

```
<?xml version="1.0" standalone="yes"?>


<UNVEvent>

<AlertId>4be9ec63-c23b-4aa0-806a-0e91d84cd33f</AlertId>

<Category>Custom</Category>
```

```
<ComputerDomain>YourCorpDomain</ComputerDomain>
<ConnectorId>fae610c9-9403-4b5e-b5d6-a81575b35f1f</ConnectorId>
<ConnectorStatus>Pending</ConnectorStatus>
<Description>evt created by Microsoft</Description>
<EventId>102</EventId>
<EventType>1</EventType>
<LastModifiedByNonConnector>11/7/2008 10:00:01 PM</LastModifiedByNonConnector>
<MaintenanceModeLastModified>1/1/1900 12:00:00 AM</MaintenanceModeLastModified>
<ManagementGroupName>YourCorpMgGrp</ManagementGroupName>
<ModifiedBy>YourCorpDomain\admin</ModifiedBy>
<MonitoringObjectId>39e8d0dc-45d2-3dc3-ace0-1731b3078218</MonitoringObjectId>
<MonitoringObjectPath>YourCorpMgGrp.YourCorpDomain.com</MonitoringObjectPath>
<MonitoringRuleId>894b1b8d-2162-62f3-a286-abd7cdcb2582</MonitoringRuleId>
<Priority>Normal</Priority>
<ProblemId>2811d1fd-1299-4f37-9c47-9b23ffa9fb1f</ProblemId>
<ResolutionState>New</ResolutionState>
<Severity>Error</Severity>
<StateLastModified>10/30/2008 5:00:01 PM</StateLastModified>
<TimeAdded>11/6/2008 7:55:23 PM</TimeAdded>
<TimeOfLastEvent>11/7/2008 10:00:01 PM</TimeOfLastEvent>
<TimeResolutionStateLastModified>11/6/2008 7:59:59 AM</TimeResolutionStateLastModified>
</UNVEvent>
```

Properties Text File Format

The following is a sample Operations Manager 2007 R2 alert that is forwarded as properties in text file format to a remote system on a UNIX or Linux platform.

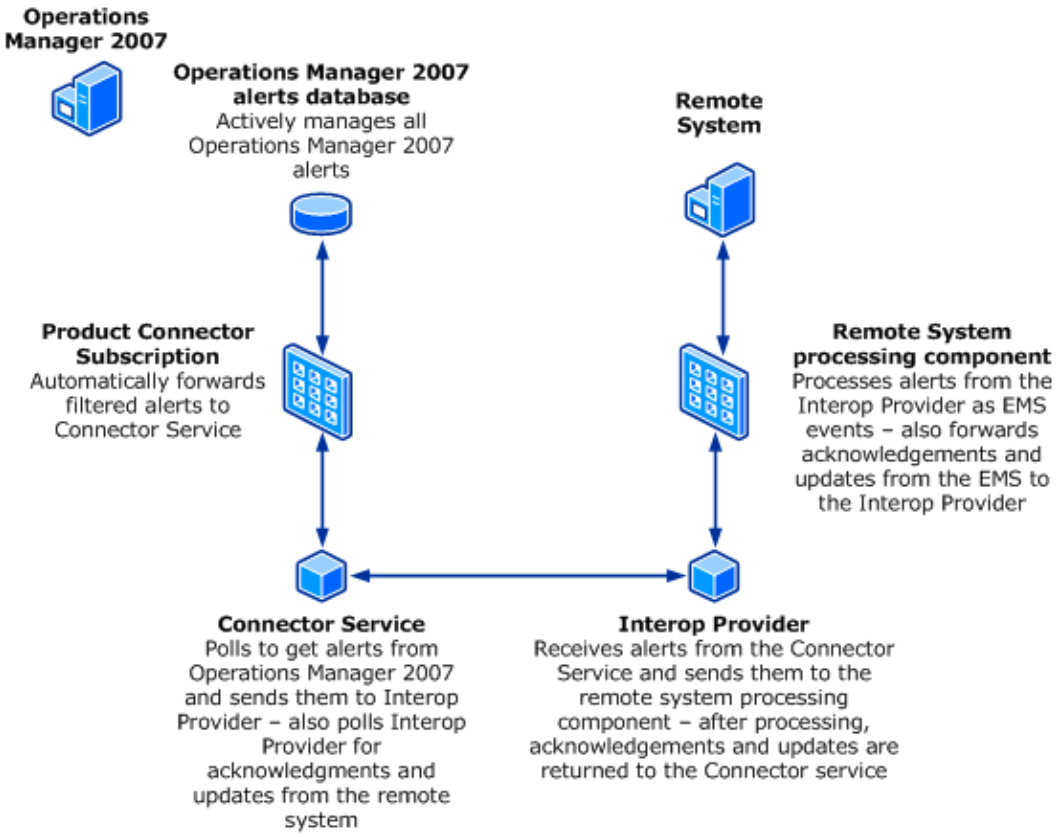
```
AlertId=1b11d523-1b91-40e3-a318-43d810d7951f
Category=Custom
ComputerDomain=YourCorpDomain
ConnectorId=fae610c9-9403-4b5e-b5d6-a81575b35f1f
ConnectorStatus=Pending
Description=evt created by Microsoft
EventId=102
```

```
EventType=1

LastModifiedByNonConnector=11/7/2008 10:00:01 PM

MaintenanceModeLastModified=1/1/1900 12:00:00 AM

ManagementGroupName=YourCorpMgGrp

ModifiedBy=YourCorpDomain \admin

MonitoringObjectId=39e8d0dc-45d2-3dc3-ace0-1731b3078218

MonitoringObjectPath=OpsMgr01.YourCorpDomain.com

MonitoringRuleId=894b1b8d-2162-62f3-a286-abd7cdcb2582

Priority=Normal

ProblemId=d2ff0b6b-c27e-477f-bb05-a3d2988387af

ResolutionState=New

Severity=Error

StateLastModified=10/30/2008 5:00:01 PM

TimeAdded=11/6/2008 7:55:23 AM

TimeOfLastEvent=11/7/2008 10:00:01 PM

TimeResolutionStateLastModified=11/6/2008 7:59:59 AM
```

Controlling Connector Forwarding

This section includes information about controlling the sending and receiving activity of Operations Manager 2007 R2 Connector.

Communications flow in the Interop Connectors environment



The following procedure provides information for manually forwarding individual alerts or groups of Operations Manager 2007 R2 alerts. Use an Operations Manager 2007 R2 Product Connector subscription to configure automatic forwarding of Operations Manager 2007 R2 alerts.

To manually forward an Operations Manager 2007 alert

1. With an alert in the Results Pane of the Operations Manager 2007 R2 Operations console, right-click the alert, click **Forward to**, and then click the specific Connector you want to use.

   Note

   Multiple alerts can be selected for forwarding by using the usual methods of selecting multiple items. Use the Shift key for sequential selection or the Ctrl key for out-of-sequence selection.

2. The forwarding status of the alert that is being forwarded briefly turns to **Forwarding Pending** and then to **Successfully Forwarded**. In Operations Manager 2007 R2 the remote system event ID is stored in the Operations Manager 2007 R2 TicketID field after a successful forwarding.

Using the Operations Manager 2007 R2 Product Connector Subscription Wizard

Use the **Product Connector Properties** dialog box to access the Product Connector Subscription Wizard. This dialog box is available from the Operations Manager 2007 R2 console. The Product Connector Subscription Wizard enables automatic forwarding of Operations Manager 2007 R2 alerts. The wizard also enables you to qualify the alerts you want to send to a specific Connector for a given remote system.

Important

- Diligent use of subscription filtering is necessary when multiple Connectors are installed and automatically forwarded in a single Operations Manager 2007 R2 management group. If appropriate filtering is not configured in such a case, there is no guarantee of alert forwarding data integrity. Subscriptions should not overlap.
- When an alert is forwarded to another remote system with an Operations Manager 2007 R2 Connector, an acknowledgement is returned from that remote system containing the event ID that is known to that remote system. The ID is then stored in the TicketID field for that alert in the Operations Manager 2007 R2 alert database. Thus, if an individual alert is forwarded to more than one remote system, data for that alert can become corrupted or unreliable.
- When you define a subscription for a given Connector in a multiple Connectors environment, use especially the **Groups** or the **Targets** pages, or both, of the Product Connector Subscription Wizard to separate the alerts that are forwarded with each Connector.

To open the Product Connector Properties dialog box and access the Product Connector Subscription Wizard

1. Log on to the computer with an account that is a member of the Operations Manager Administrators role for the Operations Manager 2007 R2 management group.
2. In the Operations Manager 2007 R2 Operations console navigation pane, click **Administration**.
3. In the **Administration** navigation pane, click **Internal Connectors**.
4. All installed Connector services that are running appear in the **Internal Connectors** pane. Double-click the Connector for which you want to set a subscription, or right-click the Connector, and then click **Properties**.
5. The **Product Connector Properties** dialog box appears. In the **Subscriptions** section, click **Add** to start the Product Connector Subscription Wizard.

   Important

   When you configure a subscription with the Product Connectors Subscription Wizard, it is best not to forward **Closed** alerts. Forwarding closed alerts can cause an unexpected amount of forwarded alerts. On the **Criteria** page of the

Product Connectors Subscription Wizard, **Closed** might be checked by default, so ensure that you clear **Closed**.

To use the Product Connector Subscription Wizard

1. After you start the Product Connector Subscription Wizard, on the **General** page, type a name and a short description for the subscription you are creating, and then click **Next**.
2. On the **Groups** page, filter by groups which alerts this Connector forwards to the remote system. By default, all check boxes are selected, so alerts from all groups are forwarded. To enable the child check boxes, clear the top-level check box. After you make your selections, click **Next**.
3. On the **Targets** page, you can filter which alerts this connector forwards based on object type. By default, alerts are accepted from all object types in all management packs. You can specify particular management packs or certain monitored objects from which you want to forward alerts. To accept alerts from only specified types of objects, select **Forward alerts from targets explicitly added to the 'Approved targets' grid are approved**, and then click **Add** to select individual targets.
4. On the **Criteria** page, you can filter which alerts this connector forwards based on the severity, priority, resolution state, and category of the alert. By default, only Error severity, High and Medium priority, and both New and Closed resolution states are checked. By default, all categories are checked. However, you can individually configure all these factors to determine the criteria for alerts to be forwarded.

   After you make your selections, click **Create** to create the connector subscription. When it is created, the subscription immediately begins forwarding the subscribed alerts to the Operations Manager 2007 R2 forwarding queue, where the Connector service sends the alerts to the remote system. Subscriptions appear in the **Subscriptions** screen of the **Product Connectors** pane, when the pane is refreshed. Double-click a subscription to edit the subscription.

Stopping or Starting Connector Services

The Connector service is started automatically when it is installed. For stopping and starting the Connector service, use the Services screen on the server on which the Connector service is installed.

The Interop Provider that is installed on Windows in the remote system environment runs within Windows Management Instrumentation (WMI). WMI automatically controls the Interop Provider operation. On UNIX systems, the Interop Provider daemons start automatically when installation is complete.

To start or stop the Connector service

1. Open the **Control Panel**, open **Administrative Tools**, and then select **Services**.

2. In the **Services** list, right-click the Operations Manager 2007 R2 Connector that you want to control, and then click **Start** or **Stop**.
3. For HP Operations Manager, there is a second service, **System Center OpsMgr Event Consumer for HP OpenView**, installed in Windows to be started or stopped in the **Services** list.

To start or stop the Interop Provider on UNIX

1. The **cimserver** daemon can be started or stopped on AIX, Solaris, and HP-UX by running Scxadmin.exe from the command line. The file, Scxadmin.exe, can be found on the server on which the Interop Provider is running, in the Interop Provider installation directory.

   `scxadmin <REQUIRED-PROPERTIES>`

   <REQUIRED-PROPERTIES>

   `ACTION=`"*<action>*" – an enumerated type specifying the wanted state of the daemon. Accepted values are "-start", "-stop", "-restart", and "-status".

   `DAEMON=`"*<daemon>*" – an enumerated type specifying the affected daemon. Accepted values are "all", "cimom", and "provider"] .

2. The **scinteropd** daemon is part of **ovstart** for HP Operations Manager. It starts or stops with **ovstart** or **ovstop**—for example:

   ```
   ovstart scinteropd

   ovstop scinteropd
   ```

Appendix A - The BMC Remedy ARS Connector

Configuring the BMC Remedy ARS Server

The following configurations must be done on the Remedy ARS server or servers by a Remedy ARS administrator prior to installation of the Interop Provider of the Operations Manager 2007 Connector for Remedy ARS.

Note

- If the AR System PortMapper is not enabled, the ARTCPPORT environment variable must be set to the value of the AR TCP port for the Interop Provider to communicate with the Remedy AR system. For example:
- `set ARTCPPORT =` *your-AR-TCP-port-value*

Create an Operations Manager user as follows:

Remedy ARS Version 6.3

- Login Name = opsmgr
- Last Name = Manager
- First Name = Operations
- Support Staff? = Yes
- Type = External
- Status = Busy
- AR License Type = Fixed
- Application License Type = HelpDesk-Fixed
- Group List = APP-Support

Remedy ARS Version 7.1

- Login Name = opsmgr
- First Name = Operations
- Last Name = Manager
- Client Type = Office Based Employee
- Profile Status = Enabled
- Contact Type = Tech Support
- Support Staff = Yes
- E-mail Address = (Required for user type – create generic e-mail address)
- Permissions = Incident Master (to have access to CI data-Asset Viewer will automatically be assigned) and Incident User
- User must be a member of the support group with availability set to “No”

Create Operations Manager Alert ticket categorizations:

Remedy ARS Version 6.3

- Category = “Monitoring”
- Type = “OpsMgr”
- Item = “Alert”

Remedy ARS Version 7.1

- Operational Categorization Tier 1 = “Monitoring”
- Operational Categorization Tier 2 = “OpsMgr”
- Operational Categorization Tier 3 = “Alert"

Operations Manager 2007 R2 Connectors Interface Forms and Filters for Remedy ARS

During the Interop Provider component installation in the Remedy ARS environment, a file containing the Operations Manager 2007 R2 Interface form plus other forms and filters is copied to the designated Remedy ARS Server. These Remedy ARS forms and filters must be imported to enable the flow of Operations Manager 2007 R2 alerts to Remedy ARS tickets.

The .xml file containing these forms and filters is copied to the Interop Provider installation folder. For example, the file for Remedy ARS 6.3 the following:

```
C:\Program Files\System Center Operations Manager 2007 Providers\Operations Manager 2007 Connector to BMC Remedy AR System 6.3 Provider\SCIOpsMgr2007Interface-63.xml
```

Note

Your Remedy ARS implementation might require additional Work Flow development for interpreting Operations Manager 2007 R2 alerts and updates.

To import Connector interface forms and filters

1. Log on to Remedy Administrator as admin.
2. Ensure that any existing Operations Manager Connectors forms or filters are removed. In the **Remedy Administrator – Server Window** go to Tree view, select **Forms**, and in the **Forms** pane, select and delete all forms that start with **SCI:**. Do the same in the **Filters** pane.
3. In the **Remedy Administrator – Server Window**, use the **Tools** menu, select **Import Definitions**, and then click **From Definition File**.
4. In the **Import File** dialog box, browse to and select the `SCIOpsMgr2007Interface-`*Remedy-version*`.xml` file. To find an .xml file, ensure that the **Files of type** value is set to **AR XML Definition files (*.xml)**. Then click **Open**.
5. In the **Import Definitions** dialog box, click **Add All** to move all forms and filters to the **Objects to Import** and then click **Import** at the bottom of the dialog box.

Appendix B - The HP Operations Manager Connector

Managed Nodes in HP Operations Manager

HP Operations Manager (formerly called OpenView Operations) only displays events that are associated with nodes managed in HP Operations Manager. The Operations Manager 2007 R2 Connector for HP Operations Manager passes the node name that is associated with the event to

HP Operations Manager. If the node is not managed in HP Operations Manager, the event is dropped and is not displayed in the HP Operations Manager console. Each Operations Manager 2007 R2 node that is to be managed in HP Operations Manager must be added to HP Operations Manager.

For information about adding nodes and node management, see the HP Operations Manager user documentation.

Appendix C - The IBM Tivoli Enterprise Console Connector

How to Configure IBM Tivoli Enterprise Console to Display Events from Operations Manager 2007

You must either run the **System_Center_Interop_Configure_TEC** task or manually configure a Tivoli rule base on the IBM Tivoli Enterprise Console server for it to accept alerts from Operations Manager 2007 R2. The following procedures provide steps for doing this on an IBM Tivoli Enterprise Console server. These procedures must be run from a command prompt on either a Windows operating system or a UNIX system that has the IBM Tivoli Enterprise Console installed.

The Interop Provider component of the Operations Manager 2007 R2 Connector for IBM Tivoli Enterprise Console must be installed before you proceed with the following procedures.

Important

You must configure the Tivoli environment as noted in the first procedure before you run the **System_Center_Interop_Configure_TEC Task** or before you manually configure a Tivoli Rule Base.

To configure the Tivoli environment

1. Open a Command Prompt window and run the following.

   For Windows operating systems:

   ```
   \Windows\system32\drivers\etc\Tivoli\setup_env.cmd
   ```

   For UNIX systems:

   ```
   ./etc/Tivoli/setup_env.sh
   ```

2. Run the **bash** command to invoke the Bourne Again shell interpreter.
3. Run the following at the command prompt to set up the Tivoli environment.

   For Windows operating systems:

   ```
   . /profile_sci
   ```

   For UNIX systems:

```
. /.profile_sci
```

To run the System_Center_Interop_Configure_TEC Task

- Use the wruntask command with the following syntax.

```
wruntask –t System_Center_Interop_Configure_TEC –l  "System Center Interop
TEC Tasks" –h <TEC Server Managed Node Name> –a <RuleBase Name> –a {ACTIVE |
EXISTING | NOCLONE} –a {<RuleBase to Clone> | "_unchanged_"} –a {Y | N} –m
900
```

Where:

<TEC Server Managed Node Name> – is the name of the IBM Tivoli Enterprise Console server.

<RuleBase Name> – is the name you want to apply to your new Tivoli Rule Base.

1st –a option – is the name of an existing or new Rule Base to update or create.

2nd –a option – specifies which Rule Base to clone from.

ACTIVE – uses the currently active Tivoli Rule Base.
EXISTING – uses a configured Tivoli Rule Base.
NOCLONE – creates a new Rule Base.

3rd –a option – is the name of the existing Rule Base to clone from if EXISTING was set in the 2nd –a option. If the 2nd –a option was set to ACTIVE or NOCLONE, enter the string "_unchanged_".

4th –a option – enter Y or N to restart (Y) or not restart (N) the IBM Tivoli Enterprise Console server. If you do not restart the IBM Tivoli Enterprise Console server, the new Rule Base will not be active and Operations Manager alerts from the Connector will not appear.

-m – enter a value in seconds for the timeout period.

The following is an example of the wruntask command using the currently active rule base to clone.

```
wruntask –t System_Center_Interop_Configure_TEC –l  "System Center Interop
TEC Tasks" –h myTECServer –a myRuleBase –a ACTIVE –a "_unchanged_" –a Y –m
900
```

To manually configure a Tivoli rule base

1. Import the class file to define the event classes that are used by the Operations Manager 2007 R2 Connector for IBM Tivoli Enterprise Console by typing the following:

```
wrb –imprbclass $SCI_HOME/Tivoli/SCInterop.baroc <rule base name>
```

Note

The rule base name should be an existing rule base (for example, **sci_OpsMgr2007toTEC**). If you must create a new rule base, use the command

wrb –crtrb <rule base name>.

2. Import the rules to define the processing for the Operations Manager 2007 R2 Connector for IBM Tivoli Enterprise Console classes by typing:

   ```
   wrb –imprbrule $SCI_HOME/Tivoli/SCInteropTEC.rls <rule base name>
   ```

3. Import the rules into the rule base target by typing:

   ```
   wrb –imptgtrule SCInterop <target – often it is "EventServer"><rule base
   name>
   ```

4. Compile the rule base by typing the following (the { } brackets are syntax noting `–trace` as optional):

   ```
   wrb –comprules {-trace} <rule base name>
   ```

5. Load the rule base by typing:

   ```
   wrb –loadrb –use <rule base name>
   ```

6. Stop the IBM Tivoli Enterprise Console Server: **wstopesvr**
7. Start the IBM Tivoli Enterprise Console Server: **wstartesvr**
8. Copy the **sciCreateTECEvtFile.sh** file to the IBM Tivoli Enterprise Console scripts directory. The following example assumes default directories:

   ```
   cp $SCI_HOME/Tivoli/sciCreateTECEvtFile.sh $BINDIR/TME/TEC/scripts
   ```

Appendix D - The Universal Connector

Examples for Alert Message Integration Logic

As noted in the Using the Universal Connector section, integration logic must be developed to translate and transfer the alert message content, as saved by the Interop Provider, to the remote system that the Universal Connector is serving. The following are examples of Windows PowerShell script that can serve as a starting point in this task. In these samples the remote system is designated as the EMS Emulator.

Script for processing a new alert

```
#  Copyright (c) Microsoft Corporation.  All rights reserved.
#
#  For personal use only.
#  Provided AS IS and WITH ALL FAULTS.
#
# Sample script to process incoming alerts from SCOM 2007 R2
# forwarded via the Universal Connector.
```

```
#

## Path to alert xml files forwarded from OpsMgr
$FromOMPath="C:\Program Files\System Center Operations Manager 2007 Providers\Operations
Manager 2007 Connector to Microsoft Universal Provider\UnvEvents\FromOpsMgr"

## Path to EMS Emulator
$EMSPath="C:\Program Files\EMSEmulator"

## Path to xml files to be sent to OpsMgr
$ToOMPath = "C:\Program Files\System Center Operations Manager 2007 Providers\Operations
Manager 2007 Connector to Microsoft Universal Provider\UnvEvents\"

## Next Ticket Number from EMS EMulator Config
$EMSConfigFile=$EMSPath + "\config\EMSEmulatorConfig.xml"
$EMSConfigxml = [xml] (get-content $EMSConfigFile)
$NextTicket = [int] $EMSConfigxml.EMSConfig.NextTicket

## Read alert xml files from OpsMgr
$alertfiles = (get-childitem -path $FromOMPath -include *.xml -recurse)

foreach($alertfile in $alertfiles) {
$xml= [xml](get-content $alertfile)

# New Alert Processing - EventType = 0
if ($xml.UNVEvent.EventType = "0") {

# ADD Logic to Insert alert into Customer Application
# simulation follows
$newelem = $xml.CreateElement("TicketNumber")
$newelem.set_InnerText($NextTicket)
$xml.UNVEvent.AppendChild($newelem)
$newFile=$EMSPath + "\" + $NextTicket + ".xml"
$xml.save($newFile)
```

```
# CREATE Acknowledgement for New Alert, return TicketNumber
$ackxml = new-object System.Xml.XmlDocument

# Create root node
$ackroot = $ackxml.CreateElement("UNVEvent")
$ackxml.appendchild($ackroot)

# Add EventType to ackxml
$ackelem = $ackxml.CreateElement("EventType")
$ackelem.set_InnerText("2")
$ackroot.AppendChild($ackelem)

# Add AlertId to ackxml
$ackelem = $ackxml.CreateElement("AlertId")
$ackelem.set_InnerText($xml.UNVEvent.AlertId)
$ackroot.AppendChild($ackelem)

# Add EventID to ackxml
$ackelem = $ackxml.CreateElement("EventId")
$ackelem.set_InnerText($NextTicket)
$ackroot.AppendChild($ackelem)

# Add ManagementGroup to ackxml
$ackelem = $ackxml.CreateElement("ManagementGroupName")
$ackelem.set_InnerText($xml.UNVEvent.ManagementGroupName)
$ackroot.AppendChild($ackelem)

# Add xml intro
$xmlintro = $ackxml.CreateProcessingInstruction("xml", "version='1.0'")
$ackxml.InsertBefore($xmlintro, $ackroot)

# Check for MgmtGroup directory, create if it doesn't exist
$MGdir = $ToOMPath + $xml.UNVEvent.ManagementGroupName
```

```
$ackFile = $MGdir + "\" + $NextTicket + ".xml"

if (!(Test-Path $MGdir)) { mkdir $MGdir }

$ackxml.save($ackFile)

remove-item $alertfile

$NextTicket++
}

}

# update EMS Config File with new NextTicket value
$EMSConfigxml.EMSConfig.NextTicket = [string] $NextTicket
$EMSConfigxml.save($EMSConfigFile)
```

Script for processing an Operations Manager alert update

```
#  Copyright (c) Microsoft Corporation.  All rights reserved.
#
#  Not for commercial use.
#
# Sample script to process incoming alerts updates from Operations Manager 2007 R2
# forwarded via the Universal Connector.
#

## Path to alert xml files forwarded from OpsMgr
$FromOMPath="C:\Program Files\System Center Operations Manager 2007 Providers\Operations
Manager 2007 Connector to Microsoft Universal Provider\UnvEvents\FromOpsMgr"

## Path to EMS Emulator
$EMSPath="C:\Program Files\EMSEmulator"
```

```
## Path to xml files to be sent to OpsMgr
$ToOMPath = "C:\Program Files\System Center Operations Manager 2007 Providers\Operations
Manager 2007 Connector to Microsoft Universal Provider\UnvEvents\"

## Read alert xml files from OpsMgr
$alertfiles = (get-childitem -path $FromOMPath -include *.xml -recurse)

foreach($alertfile in $alertfiles) {
$xml= [xml](get-content $alertfile)

# Alert Update Processing - EventType = 1
if ($xml.UNVEvent.EventType = "1") {

# ADD Logic to Update the Customer Application with data from OpsMgr
# simulation follows
# Find Ticket that matches the one from the update
$EMSfilename = $EMSPath + "\" + $xml.UNVEvent.EventId + ".xml"
if ((Test-Path $EMSfilename)) {
# Get matched Ticket
$existingTicket = [xml] (Get-Content $EMSfilename)

# Update Resolution State
 $existingTicket.UNVEvent.ResolutionState = $xml.UNVEvent.ResolutionState
$existingTicket.save($EMSfilename)

}

# CREATE Acknowledgement for New Alert, return TicketNumber
$ackxml = new-object System.Xml.XmlDocument

# Create root node
$ackroot = $ackxml.CreateElement("UNVEvent")
$ackxml.appendchild($ackroot)
```

```
# Add EventType to ackxml
$ackelem = $ackxml.CreateElement("EventType")
$ackelem.set_InnerText("3")
$ackroot.AppendChild($ackelem)

# Add AlertId to ackxml
$ackelem = $ackxml.CreateElement("AlertId")
$ackelem.set_InnerText($xml.UNVEvent.AlertId)
$ackroot.AppendChild($ackelem)

# Add EventID to ackxml
$ackelem = $ackxml.CreateElement("EventId")
$ackelem.set_InnerText($xml.UNVEvent.EventId)
$ackroot.AppendChild($ackelem)

# Add ManagementGroup to ackxml
$ackelem = $ackxml.CreateElement("ManagementGroupName")
$ackelem.set_InnerText($xml.UNVEvent.ManagementGroupName)
$ackroot.AppendChild($ackelem)

# Add xml intro
$xmlintro = $ackxml.CreateProcessingInstruction("xml", "version='1.0'")
$ackxml.InsertBefore($xmlintro, $ackroot)

# Check for MgmtGroup directory, create if it doesn't exist
$MGdir = $ToOMPath + $xml.UNVEvent.ManagementGroupName
$ackFile = $MGdir + "\" + $xml.UNVEvent.EventId + ".xml"

if (!(Test-Path $MGdir)) { mkdir $MGdir }

$ackxml.save($ackFile)

remove-item $alertfile
```

```
}

}
```

Script for processing a remote system update to Operations Manager

```
#  Copyright (c) Microsoft Corporation.  All rights reserved.
#
#  For personal use only.
#  Provided AS IS and WITH ALL FAULTS.
#
# Sample script to simulate the closing of a ticket in the EMS Emulator and
# create the necessary file to close the corresponding alert in OpsMgr
#
#
param($CloseTicket)

## Path to alert xml files forwarded from OpsMgr
$FromOMPath="C:\Program Files\System Center Operations Manager 2007 Providers\Operations
Manager 2007 Connector to Microsoft Universal Provider\UnvEvents\FromOpsMgr"

## Path to EMS Emulator
$EMSPath="C:\Program Files\EMSEmulator"

## Path to xml files to be sent to OpsMgr
$ToOMPath = "C:\Program Files\System Center Operations Manager 2007 Providers\Operations
Manager 2007 Connector to Microsoft Universal Provider\UnvEvents\"

## Ticket Number to close
#$CloseTicket=$arg[0]

# Simulate the closing of a Ticket in the EMS
```

```
# ADD Logic to Update the Customer Application with data from OpsMgr
# simulation follows
# Find Ticket that matches the one from the update
$EMSfilename = $EMSPath + "\" + $CloseTicket + ".xml"
if ((Test-Path $EMSfilename)) {
# Get matched Ticket
$existingTicket = [xml] (Get-Content $EMSfilename)

# Update Resolution State
$existingTicket.UNVEvent.ResolutionState = "Closed"
$existingTicket.save($EMSfilename)

# Need to Create file to be picked up by Connector and close OpsMgr alert
$closexml = new-object System.Xml.XmlDocument

# Create root node
$closeroot = $closexml.CreateElement("UNVEvent")
$closexml.appendchild($closeroot)

# Add EventType to closexml
$closeelem = $closexml.CreateElement("EventType")
$closeelem.set_InnerText("1")
$closeroot.AppendChild($closeelem)

# Add AlertId to closexml
$closeelem = $closexml.CreateElement("AlertId")
$closeelem.set_InnerText($existingTicket.UNVEvent.AlertId)
$closeroot.AppendChild($closeelem)

# Add ManagementGroup to closexml
$closeelem = $closexml.CreateElement("ManagementGroupName")
$closeelem.set_InnerText($existingTicket.UNVEvent.ManagementGroupName)
$closeroot.AppendChild($closeelem)
```

```
# Add ResolutionStateto closexml
$closeelem = $closexml.CreateElement("ResolutionState")
$closeelem.set_InnerText($existingTicket.UNVEvent.ResolutionState)
$closeroot.AppendChild($closeelem)

# Add xml intro
$closeintro = $closexml.CreateProcessingInstruction("xml", "version='1.0'")
$closexml.InsertBefore($closeintro, $closeroot)

# Check for MgmtGroup directory, create if it doesn't exist
$MGdir = $ToOMPath + $existingTicket.UNVEvent.ManagementGroupName
$closeFile = $MGdir + "\" + $existingTicket.UNVEvent.TicketNumber + ".xml"

if (!(Test-Path $MGdir)) { mkdir $MGdir }

$closexml.save($closeFile)

}
```