IBM WebSphere Application Server Version 7.0

Centralized Installation Manager for IBM WebSphere Application Server Network Deployment Version 7.0

Note:

Before using this information, be sure to read the general information under Appendix C: Notices.

CONTENTS

1 Introduction

The centralized installation manager (CIM) is a new feature for WebSphere® Application Server Network Deployment, Version 7.0 for distributed platforms, IBM® i (previously known as i5/OS®), and Windows® operating systems. Use this feature to simplify the installation and update of machines within a Network Deployment cell. With this feature, the cell administrator only has to install Network Deployment on one machine and create a deployment manager node. After you start the deployment manager, the cell administrator can use CIM to perform the following operations through the WebSphere administrative console or **wsadmin** command-line tool:

1. Install WebSphere Application Server Network Deployment, Version 7.0 on target hosts running one of the supported platforms; create a managed profile and federate the newly created node to the cell.

2. Install WebSphere Application Server Network Deployment, Version 7.0 customized installation package (CIP) on target hosts running one of the supported platforms; create a managed profile and federate the newly created node to the cell.

3. Download interim fixes and fix packs from the IBM support site directly to the centralized installation manager repository.

4. Install interim fixes and fix packs for WebSphere Application Server Network Deployment, Version 7.0 on target nodes that are within the Network Deployment cell.

5. Install interim fixes and fix packs for WebSphere Application Server Network Deployment, Version 6.1 on target nodes that are within the Network Deployment cell. This is a mixed-version cell where the deployment manager node is a Version 7.0 node.

This document describes each of the previous tasks in details, including how to create the centralized installation manager repository and populate the repository with installation binary files for installation to remote targets.

The target audience of this document is the system administrator or cell administrator responsible for installing WebSphere Application Server code and maintenance to hosts that are part of the Network Deployment cell.

This feature does not replace the standard installer and update installer tool used to install and update the WebSphere Application Server product. Rather, the centralized installation manager pushes the product binary files or maintenance to the remote targets and invokes the standard installer or update installer tool to perform the installation or update on the targets.

Relationship to the centralized installation manager in WebSphere Extended Deployment

This feature was originally supported in WebSphere Virtual Enterprise as part of the WebSphere Extended Deployment, Version 6.1 family of products. For WebSphere Application Server Version 7.0, the centralized installation manager was extended to support the installation and maintenance of WebSphere Application Server Network Deployment Version 7.0. Functions previously supported by the WebSphere Extended Deployment version of CIM are carried over to the new version. However, some of the functions that are specific to WebSphere Extended Deployment will require the installation of WebSphere Virtual Enterprise Version 6.1 on the deployment manager node that is running CIM for WebSphere Application Server Network Deployment Version 7.0.

For details on the centralized installation manager feature of the WebSphere Extended Deployment product refer to the WebSphere Virtual Enterprise, Version 6.1 Information Center (http://publib.boulder.ibm.com/infocenter/wxdinfo/v6r1/index.jsp).

Restriction: This feature is not available in WebSphere Application Server Network Deployment for z/OS®.

2 Getting started with the centralized installation manager

Use the centralized installation manager to simplify the tasks of deploying product components and installing product maintenance to your WebSphere Application Server Network Deployment Version 7.0 cell or other server environments.

Before you begin

You must first install the centralized installation manager repository on the deployment manager, and add one or more product components to the repository. Complete this task during the installation process of WebSphere Application Server Network Deployment Version 7.0. For more information, see Installing your application serving environment.

Alternatively, you can use the Installation Factory to add one or more product components to the repository. The Installation Factory is included in the WebSphere Application Server Network Deployment Version 7.0. For details, see Using the Installation Factory to add installation packages.

About this task

Use the centralized installation manager to install selected product components from its repository, which is located on the deployment manager, to the nodes. With this feature, you can shorten the number of steps that are required to create and manage your environments. You can use the centralized installation manager to complete the following actions:

Procedure

1. Install product components to one or more target workstations. See Installing Packages for more information.

2. Apply various types of maintenance to your product environment, your WebSphere Application Server Network Deployment environment, or other server environments. See Downloading the Update Installer for WebSphere Application Server Version 7.0 for more information.

3. Monitor your submitted requests by viewing the progress, completion status, and log files of each. See Monitoring requests for more information.

4. Create additional installation targets to enhance your environment, and manage any existing installation targets. See Managing installation targets for more information.

2.1 Considerations when using the centralized installation manager

As an administrator, you can remotely install or uninstall product components and maintenance to specific nodes directly from the administrative console without having to log in and repetitively perform these tasks.

The centralized installation manager does not replace the Installation wizard or the IBM® Update Installer for WebSphere Application Server. Instead, the centralized installation manager starts the Installation wizard for the product component or the Update Installer to install or uninstall the components or maintenance.

The various product components and maintenance files that you can install or uninstall by using the centralized installation manager are included in the following list:

- WebSphere Application Server Network Deployment Version 7.0
- WebSphere Application Server Version 7.0 refresh packs, fix packs, and interim fixes
- WebSphere Application Server Version 6.1 refresh packs, fix packs, interim fixes, and feature pack update
- Update Installer for WebSphere Application Server Version 7.0

See Task overview: Installing to learn more about installing or uninstalling product components or maintenance from the deployment manager and uninstalling product components when no augmented profiles exist.

See Installing the product and additional software for more information about installing and uninstalling WebSphere Application Server Network Deployment Version 7.0.

The following sections provide information to consider when using the centralized installation manager.

Starting the node agent

The centralized installation manager relies on current information regarding the versions of WebSphere Application Server that are installed on each node. This information is kept current on the deployment manager configuration by the node agent that is running on each node. The deployment manager contains the correct versions of WebSphere Application Server that are installed on each node if the node agent of each node is started at least once after each update is applied. To ensure that the deployment manager receives this information, the centralized installation manager automatically starts the node agent after each installation or uninstallation of maintenance.

Important: To locally apply updates on the nodes without using the centralized installation manager, issue the startNode command after you complete the operation to manually start the node agent.

Secondly, the centralized installation manager relies on the node agent to effectively stop the server processes on the target node and if the node agent is not running, the administrator will have to ensure that all the server processes are stopped on the target node before initiating any maintenance update operations on the node.

Update Installer for WebSphere Application Server Version 7.0

The centralized installation manager installs an appropriate level of the Update Installer on the target systems that it uses to install fix packs and other maintenance. If you had previously installed the Update Installer tool on any of the target hosts in a directory location other than `<WAS_INSTALL_ROOT>/UpdateInstaller`, then you may want to consider uninstalling the Update Installer by using its uninstallation process because that copy would not be used by the centralized installation manager. But it is not mandatory to uninstall that copy for CIM to work properly.

The centralized installation manager will automatically install the Update Installer tool (if it is not already installed in `<WAS_INSTALL_ROOT>/UpdateInstaller`) when you install fix packs or other maintenance on the target systems. If the version of the Update Installer tool found in `<WAS_INSTALL_ROOT>/UpdateInstaller` does not meet the minimum version required by the interim fix or fix pack, the centralized installation manager automatically installs a newer version on the targets, if you have downloaded the newer version of the Update Installer tool to your repository.

Lastly, you cannot use centralized installation manger to install the Update Installer on nodes that are not federated to the deployment manager cell.

For more information, see Downloading the Update Installer for WebSphere Application Server Version 7.0.

Temporary installation locations

After the centralized installation manager successfully completes the installation process on a remote node, it then deletes the installation image files that are located in the temporary location that you specify during the installation process. If the installation is unsuccessful, the files remain in the temporary location for you to use to determine what caused the installation error. However, you can safely delete the files.

2.2 Adding the installation package as part of the installation flow

You can add the installation package to the centralized installation manager repository as part of the installation flow. This function is only available in the Installation wizard of IBM WebSphere Application Server Network Deployment.

See section 2.3 for information on how to use the WebSphere Installation Factory tool to add installation packages to the centralized installation manager repository.

Before you begin

To populate the repository, ensure that you have write permission to the repository directory.

Procedure

1. Launch the Installation wizard for WebSphere Application Server Network Deployment.

2. The repository for centralized installation manager panel will be displayed after WebSphere Application Server Environments panel, only if the selected profile types are cell, deployment manager or none.

3. To create a repository, select the **Create a repository for Centralized Installation Managers** check box.

    a. Click **Browse** to specify the directory path of the repository.

    b. Select **Populate the repository with this installation package** check box to populate the repository.

    c. Finally, click **Next** to continue.

    If you did not select the check box, use the WebSphere Installation Factory to create and populate a repository later.

4. If the directory path of repository already contains the same installation package, the option dialog is displayed. Click **Yes** to overwrite the existing installation package. Click **No** otherwise.

Silent installation

Use the following optional parameters to create and populate a CIM repository:

- `-OPT cimSelected="`*true*"

  Specify this option to create a repository for centralized installation managers.

- `-OPT cimRepositoryLocation="`*installation_location/cimgr*"

  This option must be specified if cimSelected option is specified.

- -OPT populateRepository="*true*"

  Specify this option to populate the repository with the current installation package.

- -OPT overwriteRepository="*true*"

  Specify this option to overwrite the existing installation package.

Example 1:

Use these options to create and populate the repository with the installation package on /opt/IBM/WebSphere/cimrepos, and overwrite the existing installation package.

-OPT cimSelected="*true*"
-OPT cimRepositoryLocation="*/opt/IBM/WebSphere/cimrepos*"
-OPT populateRepository="*true*"
-OPT overwriteRepository="*true*"

Example 2:

If the specified installation package already exists in the repository, then use these options to create the repository on /opt/IBM/WebSphere/cimrepos only. Otherwise, these options create and populate the repository with the installation package.

-OPT cimSelected="*true*"
-OPT cimRepositoryLocation="*/opt/IBM/WebSphere/cimrepos*"
-OPT populateRepository="*true*"
-OPT overwriteRepository="*false*"

Example 3:

Use these options to create the repository on /opt/IBM/WebSphere/cimrepos only.

-OPT cimSelected="*true*"

-OPT cimRepositoryLocation="*/opt/IBM/WebSphere/cimrepos*"

-OPT populateRepository="*false*"

-OPT overwriteRepository="*false*"

2.3 Using the Installation Factory to add installation packages

Use the Installation Factory to add WebSphere Application Server Version 7.0 or WebSphere Application Server customized installation packages (CIP) to the repository. From the administrative console, you can then use the centralized installation manager to install your added components from the repository to the nodes.

Before you begin

To populate the repository, ensure you have write permission to the repository directory. To configure the WebSphere Application Server installation to associate with the repository, ensure you have write permission to the `<app_server_root>/`properties directory.

Procedure

1. Launch the Installation Factory from the following location:
   - Windows
     installation_factory_root`/bin/ifgui.bat`
   - AIX HP-UX Solaris Linux
     installation_factory_root`/bin/ifgui.sh`
2. Click **Manage Repository for Centralized Installation Manager**.
3. On the WebSphere Application Server installation directory page, you can optionally enter the directory path to a WebSphere Application Server installation to associate the repository with the installation. Click **Next**.
4. On the Repository and Installation Package page, enter the directory path to the repository, and enter the directory path to an installation package. Click **Next**.

The specified installation package is populated to the repository when the procedure is complete. If you only want to configure the WebSphere Application Server installation to associate the repository, then enter the directory path to the WebSphere Application Server installation on the previous page and leave the directory path to installation package to empty.

To change your selections, click **Back**.

5. Review the preview page, and click **Finish** to begin the procedure on the repository.

Command line

You can also launch the Installation Factory command line from the following location:

- Windows
  installation_factory_root`/bin/ifcli.bat`
- AIX HP-UX Solaris Linux
  installation_factory_root`/bin/ifcli.sh`

You can specify the following options:

-wasPath *wasInstallationPath*

Specifies the directory path of the WebSphere Application Server installation.

-repositoryPath *repositoryPath*

Specifies the directory path of the repository.

-installationPackagePath *installationPackagePath*

Specifies the directory path of the installation package.

-overwrite

Overwrites the existing installation package in the repository.

Use the following command to create the repository on D:\CIM\repository. If the repository does not already exist, populate the repository with the installation package on E:\WAS70ND, and configure the WebSphere Application Server installation on C:\IBM\WebSphere\AppServer with the repository.

```
ifcli.bat -wasPath C:\IBM\WebSphere\AppServer -repositoryPath
D:\CIM\repository -installationPackagePath E:\WAS70ND
```

Use the following command to add the installation package in E:\WAS70ND to the repository, which is associated with the WebSphere Application Server installation in C:\IBM\WebSphere\AppServer.

```
ifcli.bat -wasPath C:\IBM\WebSphere\AppServer -installationPackagePath
E:\WAS70ND
```

Use the following command to add the installation package in E:\WAS70ND to the repository in D:\CIM\repository. Overwrite the installation package in the repository if it exists already.

```
ifcli.bat -repositoryPath D:\CIM\repository -installationPackagePath
E:\WAS70ND -overwrite
```

Use the following command to configure the WebSphere Application Server installation in C:\IBM\WebSphere\AppServer with the repository at D:\CIM\repository. The repository is created if it does not exist.

```
ifcli.bat -wasPath C:\IBM\WebSphere\AppServer -repositoryPath
D:\CIM\repository
```

Results

The centralized installation manager repository now contains one or more WebSphere Application Server installation packages.

Each WebSphere Application Server installation has only one associated repository. The repository is shared among all the deployment managers of the installation.

Alternatively, you can add the installation package to the repository as you install the installation package on the deployment manager workstation.

2.4 Special procedures for IBM i operating systems

Special procedures are required if you choose to run Centralized Installation Manager on IBM i operating systems. Since the Installation Factory is not supported on IBM i operating system, you must create the repository on a Windows operating system and then transfer the repository to the IBM i operating system.

There are two ways to add installation packages into a CIM repository on an IBM i operating system. For local installations, the install image can be added as an optional procedure during the silent install of WebSphere Application Server. For remote installations, the user can use the Installation Factory to create a repository on a Windows system, and then transfer the packages to the repository that resides on the IBM i system.

Using the silent installer locally on IBM i operating systems

Edit the response file, and set options cimSelected, cimRepositoryLocation, and populateRepository to the appropriate values. See comments in the response file for more details. The repository is created and populated as part of the installation process. For more information, see Installing the product on IBM i operating systems.

Using the Installation Factory on Windows operating systems

1. Install WebSphere Application Server Network Deployment Version 7.0 onto the IBM i operating system.

2. Install the Installation Factory onto the Windows operating system.

3. Insert the WebSphere Application Server Network Deployment Version 7.0 installation disk into the drive of the Windows system, or create a CIP with Installation Factory on the Windows system.

4. Create a repository locally on the Windows operating system with the Installation Factory.

5. Change the directory to the repository path.

   Run: **zip -r cimrepos.zip *** to create a compressed file including all the directories in the repository.

You can also selectively include only the directories you want. If you are including any CIP images, you need to also include the corresponding CIP descriptors that are in the `descriptors` directory. The CIP descriptor is an XML file whose name contains the CIP directory name. For example, if the CIP directory name is *com.ibm.torolab.ND70_AIX_PPC32_1.0.0.0*, then the descriptor name is something like *InstallPackageND70X_com.ibm.torolab.ND70_AIX_PPC32_1.0.0.0.xml*.

6. Log onto the IBM i system.

   Open the property file, `<app_server_root>/properties/cimgr.props`, and look at the value of CENTRALIZED_INSTALL_REPOSITORY_ROOT. This is the location of the repository on the IBM i system. You can change it to point to another location.

7. Create the repository directory if it is not already created.

8. Transfer the file, cimrepos.zip, from the Windows system to the repository directory on the IBM i system. Extract the contents of the cimrepos.zip file onto the repository directory and optionally delete the file, cimrepos.zip. Now you have added the installation packages into the CIM repository on the IBM i system.

Instead of creating the repository on the disk drive of the Windows system and transferring the file, alternatively, you can map the IBM i file system of the repository onto the Windows system and use it for populating the installation packages. Using this alternative method eliminates transferring the files to the IBM i system.

What to do next

Use the centralized installation manager to install the components to the nodes and begin managing your environments. In the administrative console, click **System administration** > **Centralized Installation Manager**.

2.5 Considerations when using customized installation packages

WebSphere Application Server Version 7.0 customized installation packages

You can install WebSphere Application Server Version 7.0 customized installation packages (CIP) using centralized installation manager. For a new installation, you can either click the **Install** button or the **Install with response file** button on the Available Installation page.

For slip installation of a CIP, you must use a response file and therefore click the **Install with response file** button on the Available Installation page. After you complete a slip installation, you cannot use centralized installation manager to roll back the slip installation.

To uninstall WebSphere Application Server Version 7.0 that was installed using a customized installation image, you can select either the WebSphere Application Server Network Deployment Version 7.0 package or the WebSphere Application Server customized installation package as the installation package. Clear all features under **Select optional features**. Click the **Show Uninstallation Targets** button. Select one or more targets from the table, and click **Uninstall** to launch the wizard. Any CIP installation packages can be used to uninstall all platforms of WebSphere Application Server Version 7.0 from workstations that are part of the Network Deployment cell.

WebSphere Application Server Version 6.1 customized installation packages

Centralized installation manager does not support the installation of WebSphere Application Server Version 6.1 customized installation packages. Instead, use the fix packs to upgrade your WebSphere Application Server.

2.6 Requirements for using Remote Execution and Access

WebSphere Application Server Network Deployment provides new management features, such as initiating installations of product packages and maintenance for distributed platforms from the administrative console. To provide this new functionality, the product uses the Tivoli® Remote Execution and Access (RXA) toolkit to access your remote workstations. For this facility to work, you must complete target-specific requirements.

Windows target requirements

Many RXA operations require access to resources that are not generally accessible by standard user accounts. Therefore, the account names that you use to log onto remote Windows targets must have administrative privileges.

Simple File Sharing

Windows XP system targets must have Simple File Sharing disabled for Remote Execution and Access to work. Simple Networking requires that you log in as `guest`. A guest login does not have the authorization necessary for Remote Execution and Access to function correctly.

To disable Simple File Sharing, open Windows Explorer and click **Tools > Folder Options > View > Use Simple File Sharing**. Clear the **Use Simple File Sharing** check box. Click **Apply** and **OK**.

On Windows Vista systems, file sharing must be enabled for the Guest or Everyone accounts, and password protected sharing must be disabled. To disable password protected sharing, perform the following steps:

1. Click **Control Panel** > **Network and Sharing Center** > **Sharing and Discovery**.
2. Expand **Password protected sharing** by clicking the down arrow on the far right.
3. Select **Turn off password protected sharing**.
4. Click **Apply**, and exit the control panel.

Firewalls

Windows XP systems include a built-in firewall that is called the Internet Connection Firewall (ICF), which is disabled by default. For Windows XP Service Pack 2 systems, the Windows firewall is enabled by default. If either firewall is enabled on a Windows target workstation, Remote Execution and Access cannot access the target workstation. On Windows XP Service Pack 2, you can select the File and Printer Sharing check box in the Exceptions tab of the Windows Firewall configuration to allow access. Do not block port 445.

Administrative sharing

You must enable the remote registry administration, which is the default configuration, on the target workstation for Remote Execution and Access to run commands and scripts. To verify that the remote registry is enabled and started, click **Start > Programs > Administrative Tools > Services**. From **Remote Registry**, ensure the status of the service is started.

You must enable administrative sharing to successfully use Remote Execution and Access to connect to your Windows systems targets. Examples of the default administrative disk share are `C$` and `D$`. If you disable sharing, Remote Execution and Access considers directories that are located within the drives as hidden. In this case, the following message is displayed:

```
XCIM0009E: Error connecting to remote target <host_name>.
Exception: java.io.FileNotFoundException: CTGRI0003E The remote
path name specified cannot be found: <file_or_directory_path>.
Cause: com.starla.smb.SMBException: The network name is
incorrect.
```

To enable administrative sharing:

1. Click **My Computer**.
2. Right click the disk drive that you are enabling for administrative sharing.
3. Click **Sharing and Security**.
4. Select **Share this folder**.
5. Specify the Share name**,** such as `C$` or `D$`**,** and click **OK**.

Connecting to Windows Vista targets

To connect to Windows Vista targets, use one of the following options. Before you begin, ensure that the Remote Registry in Windows Services is started, and port 445 is unblocked in the firewall.

1. Configure both the deployment manager machine and the Vista target as members of a Windows domain. Use a user account in that domain, or in a trusted domain, when you connect to the target.

2. Enable and use the built-in administrator account to connect to the target workstation.

   To enable the built-in administrator account:

   a. Select **Control Panel > Administrative Tools > Local Security Policy > Security Settings > Local Policies > Security Options**.

   b. Next, double-click **Accounts: Administrator account status**.

   c. Select **Enable**, and click **OK**.

3. Disable the User Account Control that is enabled by default if you are using a different user account to connect to the target workstation.

   To disable User Account Control:

   a. Select **Control Panel > Administrative Tools > Local Security Policy > Security Settings > Local Policies > Security Options**.

   b. Next, double-click **User Account Control: Run all administrators in Admin Approval Mode**.

   c. Select **Disable**, and click **OK**.

Important: For the configuration changes to take effect, you must restart the workstation.

Linux and UNIX target requirements

The centralized installation manager, through RXA, uses SSH Version 2 to access UNIX® and Linux® target workstations. This usage requires the use of either OpenSSH 3.6.1 (or, if accessing AIX® targets, OpenSSH 4.7), or Sun SSH 1.1 on the target hosts.

Note that OpenSSH 3.7.1, or higher, contains security enhancements not available in earlier releases, and is recommended.

Using Secure Shell (SSH) protocol

Remote Execution and Access does not supply SSH code for UNIX operating systems. You must ensure SSH is installed and enabled on any target you want to access using CIM.

In all UNIX environments except Solaris, the Bourne shell (sh) is used as the target shell. On Solaris targets, the Korn shell (ksh) is used instead due to problems encountered with sh.

To communicate with Linux and other SSH targets using password authentication, you must edit the `/etc/ssh/sshd_config` file on the targets and set the following property:

```
PasswordAuthentication yes
```

The default value for the `PasswordAuthentication` property is `no`.

After changing this setting, stop and restart the SSH daemon using the following commands:

```
/etc/init.d/sshd stop
/etc/init.d/sshd start
```

IBM i targets

Use of SSH public/private key authentication to IBM i targets is not supported.

2.7 Additional requirement for installing or uninstalling maintenance on AIX as non-root

Before using the centralized installation manager to install or uninstall maintenance on AIX operating systems as a non-root user, you must install and configure *sudo*, which is an open-source tool, on the target AIX operating systems.

Complete the installation and configuration operations locally as the root user of the AIX operating systems without using centralized installation manager. You are required to complete the operations only once.

Procedure

1. Download sudo from the IBM AIX Toolbox Download Web site. For more information, see http://www-03.ibm.com/systems/p/os/aix/linux/toolbox/download.html.

2. Issue the following command to install sudo:

   ```
   rpm -i sudo-1.6.7p5-3.aix5.1.ppc.rpm
   ```

   You can download an AIX **installp** image for the **rpm** package manager for POWER from the previous download Web site if your AIX machine does not already have **rpm** installed.

3. Authorize a non-root user ID, which you specify, to run the **slibclean** command as a root user without providing a password. Issue the **visudo** command to add the following entry to the /etc/sudoers configuration file:

   userid `ALL = NOPASSWD: /usr/sbin/slibclean`

4. Log in with the specified user ID, and issue the **`sudo -l`** command.

   If successful, a message that is similar to the following example is displayed:

   ```
   User userid may run the following commands on this host:
   (root) NOPASSWD: /usr/sbin/slibclean
   ```

   If you do not have *sudo* installed, or *sudo* is installed but not configured correctly for the specified user ID, error messages are displayed.

3 Usage Scenarios

This section shows end-to-end use cases of how the centralized installation manager (CIM) can be used to assist WebSphere administrators.

3.1 Creating and managing a Network Deployment cell using CIM

Use the centralized installation manager (CIM) to create a WebSphere Network Deployment cell and manage it.

Before you begin

To create a multiplatform cell using the centralized installation manager (CIM), you need the following items:

1. The CDs of all the WebSphere Application Server node platforms within the cell. For example, if your cell is running on Windows, Linux and AIX operating systems, then you need the CDs for those platforms in the WebSphere Application Server Network Deployment edition.

2. The Installation Factory for WebSphere Application Server, which is available on the install tools CD. You need this CD for the platform on which your deployment manager is running.

3. For the CIM repository, you require approximately 3 GB for each platform that you have in the cell. If you plan to create custom installation packages (CIP) for use with CIM, then you must factor in additional disk space required for CIPs. You can delete images that are no longer needed from the repository to make more space available.

About this task

The centralized installation manager (CIM) is capable of creating nodes on remote hosts by installing WebSphere Application Server Network Deployment and federating them to the existing deployment manager.

Prior to CIM, you had to log in to every machine in the potential cell, install the servers manually, create a profile for each node, and federate the nodes to the deployment manager. Now, these steps are all done for you by the centralized installation manager (CIM). You only select the machine host name, and provide the login credentials.

Procedure

1. On the deployment manager machine, install WebSphere Application Server Network Deployment with management profile and deployment manager server type.

    a. Launch the WebSphere Application Server Network Deployment Installation Wizard.

    b. From the Welcome Panel, click **Next**.

    c. From the License Panel, read and agree to the terms of the license, click **Next**.

    d. From the System Prerequisite Check panel, click **Next**.

    e. From the Optional Feature Installation panel, select all features, click **Next**.

    f. From the Installation Directory panel, select a writeable folder as the WebSphere installation root, click **Next**.

    g. From the Environment Selection panel, select **Management**, click **Next**.

    h. From the Server Type Panel, select **Deployment Manager**, click **Next**.

    i. From the Administrative Security panel, specify a user name and password for logging to the administrative console. This need not be the same user name and password for logging into the deployment manager host. Click **Next**.

    j. From the Repository for centralized installation manager panel, select the option to create a repository and specify the repository location. Select to populate the repository with the installation package. Click **Next**.

    k. From the Installation Summary panel, click **Next**.

    l. After the installation is done, click **Next**.

2. Start the deployment manager. This can be done from the command line. From *INSTALL_ROOT*/profiles/Dmgr01/bin, enter the following command:

    Windows
    ```
    startManager.bat
    ```

    AIX HP-UX Solaris Linux
    ```
    ./startManager.sh
    ```

3. Log in to the administrative console.

4. Add other platform images for WebSphere Application Server Network Deployment to the CIM repository. Refer to Using the Installation Factory to add installation packages for more details.

5. Launch installations of WebSphere Application Server Network Deployment on the remote machines. Refer to Installing Packages for more details on this step.

6. You can monitor the status of the installations using CIM. Refer to Monitoring requests for more details.

Results

The installation requests are sent via the centralized installation manager to install WebSphere application servers on the remote machines to create the cell.

What to do next

The cell is now ready for management. You can add servers, install applications, and so on.

3.2 Updating a cell to a new maintenance level

A new fix pack has been released and you want to update your cell to the new maintenance level.

Before you begin

You must use the WebSphere Update Installer (UPDI) to install the fix pack locally on the deployment manager machine first. After that you must have a cell with all the node agents started. If the node agents are not running then you must make sure all the server processes on the target host have been stopped.

About this task

Complete the following steps to update all the nodes within the cell to the new maintenance level. You do not need to access the managed nodes directly while using CIM. With the node agent running on the targets, CIM will be able to stop all the running servers on the target node, update the remote node, and then restart the node agent.

Procedure

1. Update the deployment manager node to the new maintenance level.

    a. Stop the deployment manager server.

    b. Update the deployment manager node to the maintenance level needed using the Update Installer tool.

    c. Restart the deployment manager server.

2. Log in to the administrative console.

3. Download the fix pack binary files and Update Installer tool for the platforms you need into the centralized installation manager repository. You need the fix packs and Update Installers for all the nodes in the cell. Refer to Sections 4.1 and 4.3.

4. Using the administrative console, install the new fix pack on all the nodes. You do not need to install the Update Installer tool directly on each node. CIM installs UPDI automatically if needed. Refer to section 4.3 for more details.

5. You can monitor the installation requests of the maintenance packages. Refer to Section 4.4 for more details on this step.

4 Installing packages

Use the centralized installation manager to install one or more packages to the specified target workstations.

Before you begin

To successfully install a package, you must first define an *installation target*, which is the remote workstation on which selected software packages might be installed. By default, all of the workstations that contain nodes that are defined in the cell are displayed as installation targets.

Important: The centralized installation manager does not install maintenance on the deployment manager. Instead, use the IBM Update Installer for WebSphere Software to apply maintenance to the deployment manager. For more information on downloading and installing the tool, see Downloading the Update Installer for WebSphere Application Server Version 7.0.

During the installation process, the wizard prompts you to select an authentication method which is either user name and password or Secure Shell (SSH) public/private key. If you choose to use the SSH public/private key method, you must first create a pair of public/private keys and install the public key on all the installation targets. See Installing the Secure Shell public key to access your remote workstations for details.

Ensure that the centralized installation manager repository is populated with the installation image for the components that you want to install on the remote workstations. For more information on the steps to populate the centralized installation manager repository, refer to Adding the installation package as part of the installation flow and Using the Installation Factory to add installation packages.

You must first create the repository to use the features of the centralized installation manager. If you did not create the repository during the product installation, you can still set up the centralized installation manager repository and add the binary installation images to the repository. For more information, see Using the Installation Factory to add installation packages.

About this task

The number of steps to complete this task can vary depending on the type of installation package that you choose to install.

Procedure

1. Access the wizard from the administrative console.

    a. Click **System administration > Centralized Installation Manager > Available installations**.

    b. Select a package type, which is the type of installation you want to perform. For example, you can choose to complete a product installation, or an installation that applies various types of maintenance files.

    c. Next, select an installation package. If you choose a package that includes available features, select each feature from the feature list. This list is not displayed if you choose an installation package that does not include available features.

    d. Click **Show installation targets** to populate the table with a list of applicable target workstations on which to install the selected software package.

    e. Select one or more installation targets from the list, and click **Install** or **Install Using Response File** to start the Installation wizard.

    Not all installation packages support response files. The **Install Using Response File** button is disabled if that installation package does not support response files.

2. Accept the license agreement. Click **View License Agreement** to read the agreement and accept the terms. Click **Next** to continue.

3. Select an authentication method to access the installation target, and click **Next**. You can choose to use either the Secure Shell (SSH) public/private key method, or the user name and password method to authenticate.

4. Provide the authentication settings, and click **Next**.

    Depending on the authentication method that you choose in step 3, provide the appropriate user name and password for one or more installation targets, or provide the location of the SSH private key file and password on the deployment manager.

    If you choose to authenticate using the user name and password method, you can provide a common user name and password to access all of the installation targets, or you can configure unique user names and passwords for each target.

Important: Do not use the browser to save the user name and password. The browser might offer the same user name and password on different target names.

5. If you choose to install using a response file, you can click **Browse** to locate the response file in the deployment manager. For security reason, the browse function is restricted to browse response files in the <*DMGR_PROFILE_ROOT*>/cim/responsefiles directory and any subdirectories below it.

Password encoding utility program for response files

The passwords specified in the response file may optionally be encoded using the **ResponseFilePasswordEncoder** utility. The executable script files for running the utility are located in the *INSTALL_ROOT*/bin directory.

Syntax:


```
./ResponseFilePasswordEncoder.sh file_name password_keys_list
        [-Backup | -noBackup]
```


```
ResponseFilePasswordEncoder.bat file_name password_keys_list
        [-Backup | -noBackup]
```

The *password_keys_list* element is a list of password keys (delimited by comma) for which the password values are to be encoded.

The **-Backup** option is an optional argument for making a back-up copy of the response file to be encoded. The default option is **-noBackup**.

Examples:

To encode the password values in the response file, responsefile.nd.txt, identified by the keys PROF_importSigningCertKSPassword and PROF_importPersonalCertKSPassword, enter:

```
./ResponseFilePasswordEncoder.sh responsefile.nd.txt
PROF_importSigningCertKSPassword,PROF_importPersonalCertKSPassword
```

To encode the password values in the response file, responsefile.nd.txt, identified by the keys PROF_importSigningCertKSPassword and PROF_importPersonalCertKSPassword and to keep a back-up copy of the original response file, enter:

```
ResponseFilePasswordEncoder.bat responsefile.nd.txt
PROF_importSigningCertKSPassword,PROF_importPersonalCertKSPassword
-Backup
```

Invalid arguments in the command line cause the utility to display the command usage information.

6. Specify the installation location and the working location of each installation target, and click **Next**.

   The installation location is the remote location of the installation target where the package will be installed.

   The working location specifies the directory on the remote target where the centralized installation manager will transfer the binary installation files from its repository to the target for subsequent installation on the target.

   Make sure you have enough disk space on both the installation location and the working location. The space required in the installation and working location varies by installation packages. Centralized installation manager transfers the binary files for the selected installation package from the repository and extracts the content of the binary files into the working location.

7. Specify other command parameters.

   The Installation wizard is a generic wizard for all installation packages that the centralized installation manager supports. In addition to the standard installation location parameter, a particular installation package might have zero or more command parameters that require user input. Specify values for these parameters as needed or take the default values.

8. Read the installation summary, and click **Finish** to submit the installation request to the centralized installation manager for processing.

Results

You completed the steps to install one or more packages to the specified target workstations. The centralized installation manager receives your installation request, processes the information that you provided, and then installs the package to the workstations.

What to do next

In the administrative console, check the status of your pending requests on the **Installations in Progress** page, and review the log files of your submitted installation requests from the **Installation History** page. Read the details about the options that you can use to further monitor the progress of each request.

From the Installation History panel you can click **View Details** to display a panel with additional details on the results. Hyperlinks to log files on the remote targets are included. However, those logs might be moved, replaced, or deleted if they are not viewed immediately after an installation operation.

4.1 Downloading the Update Installer for WebSphere Application Server Version 7.0

Use the Update Installer for WebSphere Application Server Version 7.0 to apply and install interim fixes, refresh packs, or fix packs on remote targets for your Network Deployment environments.

Before you can use the centralized installation manager to apply maintenance to your remote workstations, you must download the latest level of the Update Installer. Use the following steps to download the Update Installer to the centralized installation manager repository.

Procedure

1. In the administrative console, click **System administration > Centralized Installation Manager > Installation Packages**.

2. Click **Update Installer for WebSphere Application Server** in the table that displays the list of installation packages.

3. Select one or more operating systems, and click **Download**.

4. Review the summary, and click **Download** to start downloading the Update Installer for the selected operating systems.

5. You can monitor the download status of the files from the **Installation Packages** panel after the download process begins. Click the icon to refresh the contents of the table, if necessary.

6. Check for error messages from `<INSTALL_ROOT>/profiles/<dmgr profile name>/logs/dmgr/SystemOut.log`, if necessary.

What to do next

When the download status of the file is displayed as completed, you can select and install the maintenance on the remote targets. You do not need to select the Update Installer and install to the targets directly. Instead, the Update Installer is automatically installed when you install a fix pack or interim fix. The centralized installation manager only installs the Update Installer on nodes that are federated to the cell.

4.2 Installing interim fixes

Install selected interim fixes to specific installation targets to update your product environment.

The centralized installation manager (CIM) relies heavily on remote node information maintained locally on the deployment manager node. This remote node information (namely the node-metadata.properties file) for each node is refreshed every time the node agent on the remote node starts and provides the centralized installation manger with up-to-date information regarding the WebSphere products and versions that are installed on the target nodes.

One example of how the node-metadata.properties information is being used by the centralized installation manager is in the filtering of nodes that might be selected for the installation of an interim fix.

Assume you have downloaded an interim fix for the Feature Pack for Web Services to the centralized installation manager repository to be installed on remote node. CIM looks at the information contained within the interim fix and determines that the fix is only applicable for nodes that have the Feature Pack for Web Services Version 6.1.0.9 or higher installed. CIM then checks the node-metadata.properties of all the nodes within the cell to determine which of the remote nodes meet the requirement for this interim fix. This process allows the cell administrator to see which nodes are potential candidates for this update and then initiate the installation of the interim fix on one or all the candidate nodes. Because of the availability of the node-metadata.properties on the deployment manager node, you could use CIM to perform this filtering without accessing the target nodes. The node agent process that runs on each node ensures that the node-metadata.properties files of the nodes on the deployment manager are kept up-to-date.

For this reason, if you apply maintenance to the node or install new WebSphere products (such as the Feature Pack for Web Services) outside of CIM on the remote node, you must restart the node agent process after the installation to get the deployment manager copy of the node-metadata.properties of the node up-to-date.

In addition, for the case of installing a new WebSphere product on the remote 6.1 nodes you **must** take one of the following two steps:

1. If the product you are installing supports profile augmentation, augment an existing profile for an already federated node.

2. If the product you are installing does not support augmenting an existing profile or you prefer not to augment an existing profile, then create a new profile using a profile template for the new product (for example, a Feature Pack for Web Services profile) thereby creating a new node. Federate this new node to the current deployment manager cell.

After the profile is augmented or a new one is created and federated to the cell, the node agent must be started to make the updated or new node-metadata.properties file that contains the new product information available to the deployment manager node. Unless this is done, CIM, running on the deployment manager node, has no knowledge of the new product that has been installed on the remote host and cannot perform the filtering correctly.

Before you begin

You must download the following items to the centralized installation manager repository before you can complete this task:

- IBM Update Installer for WebSphere Application Server Version 7.0
- The binary files for one or more interim fixes

You do not need to install the Update Installer after you have downloaded it. The centralized installation manager automatically installs the Update Installer before installing any refresh packs, fix packs or interim fixes if the target does not have the Update Installer already installed.

The descriptors for an interim fix package type are installed when you install WebSphere Application Server Network Deployment Version 7.0. These specific descriptors are included to apply the following types of updates:

- Maintenance for WebSphere Application Server Network Deployment Version 6.1
- Maintenance for WebSphere Application Server Network Deployment Version 7.0

For details on how to locate the descriptor and associated files, see Downloading package descriptors and the associated binary files.

By default, all of the workstations containing nodes that are defined in the cell are displayed as installation targets. You can only install interim fixes on targets that are part of the cell. During the installation process, the wizard prompts you to select an authentication method, either user name and password or Secure Shell (SSH) public/private key. If you choose to use the SSH public/private key authentication method, you must first create a pair of keys and install the public key on all the installation targets to successfully complete this task.

Before installing an interim fix to any targets, you must install the same interim fix to the deployment manager first, if the interim fix is applicable to the deployment manager node.

For WebSphere Application Server Version 7.0 nodes, CIM can detect what interim fixes have been installed. If you select an interim fix that has been previously installed to a node, that node is not available for selection.

For WebSphere Application Server Version 6.1 nodes, you can still select nodes that have the interim fix installed, but you are notified that the interim fix has been previously applied on the Installation history page.

About this task

Complete the following steps to install recommended interim fixes for WebSphere Application Server Network Deployment Version 6.1 or 7.0.

Procedure

1. Access the wizard from the administrative console.

    a. Click **System administration > Centralized Installation Manager > Available installations**.

    b. Select **Interim fix** as the package type. Next, select one of the following maintenance installation packages.

    - Maintenance for WebSphere Application Server Network Deployment 7.0
    - Maintenance for WebSphere Application Server Network Deployment 6.1

    If you previously downloaded any interim fixes by using the **Installation Packages** function, the interim fixes are displayed in a list below the **Select one or more maintenance packs** prompt. Select one or more interim fixes from this list.

c. Click **Show installation targets** to populate the table with a list of applicable target workstations on which to install the selected interim fixes. After you select one or more installation targets, click **Install** to start the Installation wizard.

2. Read and accept the license agreement.

   Click **View License Agreement** to read the agreement and accept the terms. Click **Next** to continue.

3. Select an authentication method to access the installation target, and click **Next**.

   You can select to either use the Secure Shell (SSH) public/private key method or the user name and password method to authenticate.

4. Provide your authentication information, and click **Next**.

   Depending on the authentication method that you choose in the previous step, provide the appropriate user name and password for one or more installation targets, or provide the location of the SSH private key file and password on the deployment manager.

   If you choose to authenticate by using the user name and password method, you can provide a common user name and password to access all of the installation targets, or you can configure unique user names and passwords for each target.

5. Verify the installation and the working locations of each installation target, and click **Next**.

   The installation location is the remote location of each installation target in which the interim fixes are to be installed. The working location specifies the directory on the remote target where the files are sent before the package is installed in the specified location.

   Make sure you have enough disk space in both the installation location and the working location. The space required in the installation and working location varies by installation packages. The centralized installation manager transfers the selected interim fix files and the Update Installer binary file if necessary from the repository to the working location.

6. Read the installation summary, and click **Finish** to submit the installation request to the centralized installation manager for processing.

Results

Your installation request is sent to the centralized installation manager for processing. The Update Installer is automatically installed to the selected targets if the Update Installer is not found on the targets.

To check the status of your request, click **Installations in progress** in the administrative console.

The following message is displayed if you attempt to install an interim fix without having a copy of the IBM Update Installer for WebSphere Application Server Version 7.0 in your CIM repository:

```
The installation binary files required for the install_package_name or its
dependent package Update Installer for WebSphere Application Server for
<workstation_platform> do not exist.
```

What to do next

Click **Installation history** in the administrative console to review the log files for each of the installation requests that you submit.

From the Installation History panel the administrator can click **View Details** to display a panel with additional details on the results. Hyperlinks to logs on the remote targets are included. However, those logs can be moved, replaced, or deleted by other users or administrator, if they are not viewed immediately after an installation operation.

4.3 Installing refresh packs or fix packs

Install recommended fix packs or refresh packs to specific installation targets to update your product environment.

The centralized installation manager supports the installation of Network Deployment Version 6.1 fix packs on remote nodes that are within the Network Deployment cell. This configuration is known as a mixed-version cell where the deployment manager node is at Version 7.0 or higher and the other nodes within the cell are either at the same level as the deployment manager node or at the Version 6.1 level.

CIM does not support maintenance levels below Version 6.1.

CIM currently has definitions for Network Deployment Version 6.1 Fix Pack 15 and 17. When newer Network Deployment Version 6.1 Fix Packs become available, CIM will have definitions for those as well. The content of these CIM-defined Network Deployment Version 6.1 Fix Packs include the following individual fix packs for the distributed platforms and Windows:

- WebSphere Application Server fix pack
- Java™ Software Developer Kit (SDK) fix pack
- WebSphere Application Server Feature Pack for Web Services fix pack
- WebSphere Application Server Feature Pack for Enterprise JavaBeans 3.0 fix pack

For IBM i targets, the CIM-defined Network Deployment Version 6.1 Fix Packs are the same but without the Java SDK fix pack.

With the CIM-defined Network Deployment Version 6.1 Fix Packs pre-loaded in the CIM repository, the cell administrator can specify the remote nodes that the CIM-defined Network Deployment Version 6.1 Fix Pack is to be installed in. CIM determines whether any of the two Feature Pack fix packs are required and only sends the necessary ones to the target nodes for installation. Since both Network Deployment Version 6.1 Fix Pack 15 and 17 specify that a mandatory Interim Fix, PK53084, must be installed on the target if the Feature Pack for Web Services is installed, CIM also performs a check before allowing the installation of Fix Pack 15 and 17 to proceed.

CIM supports the uninstallation of the CIM-defined Network Deployment Version 6.1 Fix Pack from the target nodes, if the Fix Pack was installed through CIM and the CIM-defined Fix Packs are still in the CIM repository. Note that for uninstallation operations, CIM expects that the Update Installer tool is already installed on the target nodes. If the Fix Pack was originally installed using CIM, both of these conditions are automatically satisfied.

Lastly, CIM uses the Update Installer for WebSphere Application Server Version 7.0 to install and uninstall the CIM-defined Network Deployment Version 6.1 Fix Packs.

Before you begin

You must download the following items to the centralized installation manager repository before you can complete this task:

- IBM Update Installer for WebSphere Application Server Version 7.0
- Installation package descriptor and binary files for a refresh pack or fix pack

For details on how to locate the descriptor and associated files, see Downloading package descriptors and the associated binary files.

You do not need to install the Update Installer after you have downloaded it. The centralized installation manager automatically installs the Update Installer before installing any refresh packs, fix packs or interim fixes if the target does not have the Update Installer installed.

By default, all of the workstations containing nodes that are defined in the cell are displayed as installation targets. During the installation process, the wizard prompts you to select an authentication method, either user name and password or Secure Shell (SSH) public/private key. If you choose to use the SSH public/private key method, you must first create a pair of keys and install the public key on all the installation targets to successfully complete this task.

Before installing a refresh pack or fix pack to any targets, you must install the refresh pack or fix pack to the deployment manager first, if it is applicable. The deployment manager must have the highest level of refresh pack or fix pack in the cell.

About this task

Complete the following steps to install recommended fix packs or refresh packs for WebSphere Application Server Network Deployment Version 7.0.

Procedure

1. Access the wizard from the administrative console.

    a. Click **System administration > Centralized Installation Manager > Available installations**.

    b. Select **Refresh pack, fix pack, or maintenance tool** as the package type. Next, select the specific installation package that contains the refresh pack or fix pack that you want to install on the remote workstations.

    c. Click **Show installation targets** to populate the table with a list of applicable target workstations on which to install the selected package. After you select one or more installation targets, click **Install** to start the Installation wizard.

2. Read and accept the license agreement.

    Click **View License Agreement** to read the agreement and accept the terms. Click **Next** to continue.

3. Select an authentication method to access the installation target, and click **Next**. You can select to either use the Secure Shell (SSH) public/private key method or the user name and password method to authenticate.

4. Provide your authentication information, and click **Next**.

   Depending on the authentication method that you choose in the previous step, provide the appropriate user name and password for one or more installation targets, or provide the location of the SSH private key file and password on the deployment manager.

   If you choose to authenticate by using the user name and password method, you can provide a common user name and password to access all of the installation targets, or you can configure unique user names and passwords for each target.

5. Verify the installation and the working locations of each installation target, and click **Next**.

   The installation location is the remote location of each installation target in which the package is to be installed. The working location specifies the directory on the remote target where the files are sent before the package is installed in the specified location.

   Make sure you have enough disk space in both the installation location and the working location. The space required in the installation and working location varies by installation packages. The centralized installation manager transfers the selected refresh pack or fix pack files and the Update Installer if necessary from the repository to the working location.

6. The Update Installer on the targets is updated to the latest version from the repository automatically, if required. Clear the check box if you do not want the Update Installer on the targets to be updated.

7. Read the installation summary, and click **Finish** to submit the installation request to the centralized installation manager for processing.

   Attention: Any interim fixes that you previously installed on the remote targets is uninstalled by the Update Installer prior to installing the refresh pack or fix pack. If the refresh pack or fix pack does not include the official fixes that were included in the removed interim fixes, you must reinstall the interim fixes after you install the refresh pack or fix pack.

Results

Your installation request is sent to the centralized installation manager for processing. To check the status of your request, click **Installations in progress** in the administrative console.

What to do next

Click **Installation history** in the administrative console to review the log files for each of the installation requests that you submit.

From the Installation History panel, the administrator can click **View Details** to display a panel with additional details on the results. Hyperlinks to logs on the remote targets are included. However, those logs can be moved, replaced or deleted by other users or the administrator if they are not viewed immediately after an installation operation.

4.4 Monitoring requests

After you submit one or more requests to the centralized installation manager, you can monitor the progress of and view specific details about each installation and uninstallation request.

About this task

In the administrative console, the Installations in Progress and Installation History panels provide you with information on the status of the installation and uninstallation requests that you submit to the centralized installation manager for processing. However, each panel provides you with different options for using that information to monitor and manage your requests. The Installations in Progress panel provides you with options to view and monitor the progress of each request. You can also cancel any pending requests from this panel. From the Installation History panel, you can monitor the completion status, delete the history records, and access the error messages and log files of each completed request.

Procedure

Complete the following steps to monitor the progress of requests:

1. Click **System administration > Centralized Installation Manager > Installations in Progress** in the administrative console.

2. Review the table for specific details about each request, which are described in the following list:

    - **Host name** specifies the name of the workstation on which the request is performed.

    - **Operation** specifies the type of request, such as install, uninstall, or install SSH public key.

- **Package and Features** specifies the name of the software package and any accompanying features that make up the installation request.
- **Creation time** specifies the date and time you submit the request.
- **Status** specifies the progress of the request.

3. **Optional.** You may optionally cancel a request if it has not started**.**

   Select one or more rows from the table, and click **Cancel Pending Request** to cancel only the requests that are not yet started.

   Review the confirmation panel, and click **OK** to return to the **Installations in Progress** page.

Complete the following steps to view the completion status and details of requests:

1. Click **System administration > Centralized Installation Manager > Installation History** in the administrative console.

2. Review the table for specific details about each request.

   The table that is displayed on this page lists the same descriptive information as the table on the Installations in Progress page, except the status is displayed as one of the following completion types:

   - Succeeded
   - Failed
   - Installation completed, but errors detected
   - Uninstallation completed, but errors detected

3. Click **Remove** to delete the history records from the deployment manager.

   Review the confirmation panel, and click **Remove** again.

4. Click **View details** to view the log files and any error messages.

   A new page now displays any errors that might have occurred, and the links to the actual log content.

   a. Click the specific link to read the content of a log file.

      If you previously deleted the log files from the remote workstation, an error message is displayed. If you replace existing log files with new ones, the updated content is displayed.

   b. Click **OK** to return to the **Installation History** page.

What to do next

Return to the **Available Installations** page to resubmit a canceled or failed request, or submit a new request to the centralized installation manager.

In the case of certain failed requests, you might need to correct the error on the remote workstations before resubmitting the requests. For installations that are partially successful, examine the logs to correct the problem. You can manually complete the remaining installation steps. With this option, you do not need to resubmit the requests. Alternatively, if the failure state of the request is closer to the starting state, you can return the workstation to the starting state before you resubmit the requests.

5 Uninstalling packages

Use the centralized installation manager to uninstall a previously installed package from the target workstation.

Before you begin

The wizard prompts you to select an authentication method, either user name and password or Secure Shell (SSH) public/private key. If you choose to use the SSH public/private key method, you must first create a pair of keys and install the public key on all the installation targets.

About this task

The number of steps for this task can vary depending on the type of installation package you choose to uninstall.

Procedure

1. Access the wizard from the administrative console.

    a. Click **System administration > Centralized Installation Manager > Available installations**.

    b. Select a package type and an installation package. Depending on the package that you choose, you can choose to uninstall maintenance packs.

    c. Click **Show uninstallation targets** to populate the table with a list of applicable target workstations from which to remove the selected software package. After you select one or more uninstallation targets, click **Uninstall** to start the wizard.

2. Select an authentication method to access the installation target, and click **Next**. You can choose to use the Secure Shell (SSH) public/private key method or the user name and password method to authenticate.

3. Provide the authentication settings, and click **Next**. Depending on the authentication method that you choose in the previous step, provide the appropriate user name and password for one or more installation targets, or provide the location of the SSH private key file and password on the deployment manager.

If you choose to authenticate by using the user name and password method, you can provide a common user name and password to access all of the installation targets, or you can configure unique user names and passwords for each target. Do not use the browser to save the user name and password. The browser might offer the same user name and password on different target names.

4. Specify the installation location of each installation target, and click **Next**.

   The installation location is the remote location of the installation target in which the packages are installed.

5. Read the summary, and click **Finish** to submit the request to the centralized installation manager for processing.

Results

Your uninstallation request is sent to the centralized installation manager for processing. To check the status of your request, click **Installations in progress** in the administrative console.

What to do next

Click **Installation history** in the administrative console to review the log files for each of the uninstallation requests that you submit.

From the Installation History panel, the administrator can click **View Details** to display a panel with additional details on the results. Hyperlinks to logs on the remote targets are included. However, those logs can be moved, replaced or deleted by other users or the administrator, if they are not viewed immediately after an uninstallation operation.

6 Downloading package descriptors and the associated binary files

To enhance your product environment, download additional installation packages and maintenance files to the centralized installation manager repository to install later on the remote workstations. Use this section to manage the installation packages and maintenance files that are located in your centralized installation manager repository.

Before you begin

You must first create the centralized installation manager repository and add one or more product packages to the repository on the host workstation. Complete this task during the installation process of WebSphere® Application Server Network Deployment Version 7.0. For more information, see Adding the installation package as part of the installation flow.

Alternatively, you can use the Installation Factory to add one or more product packages to the repository. The Installation Factory is included in one of the WebSphere Application Server Network Deployment CDs, which you must install separately. For more details about the Installation Factory tool, see Using the Installation Factory to add installation packages.

About this task

From the Installation Packages panel in the administrative console, download the descriptor files and any associated binary files of new or additional installation packages to the centralized installation manager repository. You can selectively download only the binary files of the platforms that you might need from the IBM support Web site. The following list describes the four types of installation packages:

- Product installation

  This package type includes WebSphere Application Server Network Deployment Version 7.0. The descriptor and binary files for this installation type are not available to download, because the files are included during the product package.

- Refresh packs or fix packs

  You can download the binary files for this package type based on specific platforms. When a fix pack for IBM WebSphere Application Server is released, it usually comes with a fix pack for the WebSphere Application Server and a fix pack for the Java SDK. Centralized installation manager requires having both fix packs in the repository, and centralized installation manager will install both fix packs to all selected targets.

- Maintenance tool

  This package type includes the Update Installer, which is the tool that you use to apply maintenance to your WebSphere Application Server Network Deployment environments. Before you can use the centralized installation manager to apply maintenance to your remote workstations, you must download the latest level of the Update Installer.

  Important: You must use the Update Installer to install maintenance on the deployment manager. First apply maintenance to the deployment manager before you apply maintenance to the cell. Begin by using the centralized installation manager to download the required files, which are stored in the repository that you specify during the initial installation process. Alternatively, you can find the repository location in the `CENTRALIZED_INSTALL_REPOSITORY_ROOT` property in the `<app_server_root>/properties/cimgr.props` file where `<app_server_root>` is the WebSphere Application Server installation directory.

  On Windows operating systems, the value of the `CENTRALIZED_INSTALL_REPOSITORY_ROOT` property listed in the cimgr.props file might look like the following:

  ```
  C\:/Program Files/IBM/WebSphere/cimrepos
  ```

  Here, the extra '\' after the drive letter is simply an escape character.

- Interim fix

  You can search for an interim fix using its identifying Authorized Program Analysis Report (APAR) number. Specify the APAR number of the interim fix and click **Search** to display a list of files associated with the interim fix and optionally download the binary files.

Procedure

Complete the following steps to download fix pack descriptors and binary files for fix packs or interim fixes to your CIM repository:

1. In the administrative console, click **System administration > Centralized Installation Manager > Installation Packages**.

2. Click **Add Packages** to download a new installation package descriptor to the centralized installation manger repository if the descriptor is not included in the table displayed from the previous step. The **Download Descriptors** page is then displayed.

Tip: Ensure that the descriptor file for the type of package that you choose is not included as part of the product installation. The installation package descriptors that are included during the product installation are provided in the following list:

- Maintenance for WebSphere Application Server Network Deployment 6.1
- Maintenance for WebSphere Application Server Network Deployment 7.0
- Update Installer for WebSphere Application Server 7.0
- WebSphere Application Server Network Deployment 7.0

3. Select one or more descriptor files from the list, and click **Downloading**.

   After you have confirmed to download the selected descriptor files, they are displayed in the table on the **Installation Packages** panel with the text:

   `Downloading <filename>`

   Click the refresh icon to refresh the contents of the table. After the descriptor file is downloaded, the package name is displayed as a hyperlink.

   To download the binary files for the installation packages in the preceding list, click the name of the descriptor, and proceed to the next step. To download additional package descriptors from the IBM support Web site, click **Add packages**.

4. Download the binary files from the **Installation Packages** panel.

   You can download the associated binary files of the specific descriptor file that you just downloaded, or you can also download the binary files for the Interim fix package type.

   Determine the type of installation package to download by the viewing the descriptions of each type in the table. The steps to download the binary files differ, depending on the package type.

   - To download the binary files for a **refresh pack, fix pack, or maintenance tool** package type, which includes the Update Installer, complete the following steps:

     a. Click the name of the package in the table. A new page is then displayed.

     b. Select one or more platforms in the table, and click **Download**.

c. Click **Download** on the confirmation page to start downloading the binaries. After the download process begins, the previous page is then displayed, from which you can check the download status of the files in the third column of the table. Click the refresh icon to refresh the contents of the table, if necessary.

d. When all the required files have been downloaded, the download status column displays a Completed status.

   If one or more files are missing, the download status column displays an Incomplete status. In this case, you can try to download again. If your status is Incomplete, check for error messages in the `<profile_root>/logs/dmgr/SystemOut.log` file where `<profile_root>` is the profile location of the deployment manager.

- To download the binary files for an **Interim fix** package type, complete the following steps:

  a. Click the name of the package in the table. A new page is then displayed.

  b. Click **Add Files** to go to the **Download Files** page.

  c. You can type the specific APAR name (PKxxxxx), and click **Search** to navigate directly to the corresponding FTP location. You can also specify the FTP URL directly, and click **Go** from the Download Options section.

  d. Click the APAR number, select the individual maintenance files that are contained in the directory, and click **Download**. The binary files are then downloaded to the centralized installation manager repository.

  e. Click **Download** on the confirmation page to start downloading the binaries.

     After the download process begins, the previous page is then displayed, where you can check the download status of the files in third column of the table.

     Click the refresh icon to refresh the contents of the table, if necessary.

     If your status is Incomplete, check for error messages in the `<profile_root>/logs/dmgr/SystemOut.log` file where `<profile_root>` is the profile location of the deployment manager.

Results

The centralized installation manager repository now contains maintenance files to install later on the remote workstations.

6.1 Using CIM download function when the deployment manager does not have direct Internet access

The centralized installation manager (CIM) provides a download function in the administrative console to allow the cell administrator to navigate to IBM support and download the latest version of the Update Installer, fix packs and interim fixes. To use this feature, the WebSphere Application Server deployment manager node must have Internet access to the external IBM FTP server.

However, if you do not allow Internet access from your deployment manager workstation, then one solution is to set up an FTP gateway on a workstation that has internet access, point the CIM download URL to that gateway, and do the download indirectly through the gateway. The following section describes how you can set up a simple FTP gateway using a program called DeleGate. You can use other FTP gateway products with similar capability instead.

DeleGate is a multi-purpose application level gateway, or a proxy server which runs on multiple platforms (UNIX, Windows and OS/2®). See http://www.delegate.org.

The following steps are involved in setting up DeleGate Version 9.7.7 as an FTP gateway for CIM running on a deployment manager node that does not have direct access to the Internet.

- Download a copy of DeleGate from this URL:
  http://www.delegate.org/anonftp/DeleGate/download.html

- Installation on Windows operating systems involves opening and extracting the downloaded compressed file, dg9_7_7-fix1.zip, to a directory. Start DeleGate by running `dg9_7_7-fix1.exe` from the `bin` directory.

- To start **DeleGate** as an FTP Gateway for the CIM download function, use the following command on one line:

```
dg -P21 SERVER=ftp
MOUNT="/* ftp://ftp.software.ibm.com/software/websphere/*"
ADMIN=administrator@ftpgate01.mydomain.com PERMIT="*:*:*. mydomain.com"
```

Notes

1. In the above example, DeleGate is running on host ftpgate01.mydomain.com and it has direct connection to the Internet.

2. For convenience, the `dg9_7_7-fix1.exe` file is renamed to `dg.exe` so that `dg` can be used to start DeleGate.

3. The PERMIT parameter allows access from any host with the domain name, mydomain.com, to access the gateway.

4. You can add the "`-v`" option to make DeleGate run in the foreground with logging to the console to observe activities.

5. You can also run **DeleGate** using arguments loaded from a configuration file with the "`+=filename`" option with the specified file holding all the arguments (1 argument per line), for example:

```
dg +=dg.conf
```

With the previous setup, you can then replace `ftp://ftp.software.ibm.com/software/websphere` with `ftp://ftpgate01.mydomain.com` anywhere you see **Download Options** in any of the CIM download panels and be able to access the IBM Support FTP Server via the FTP gateway.

Tips: Expand the Download Options tag to reveal the FTP URL field that you need to replace. Only replace the front portion of the URL as described and keep the remaining portion of the URL String as is.

For example, if the FTP URL field shows:

ftp://ftp.software.ibm.com/software/websphere/appserv/support/fixpacks/was61/cumulative/

Replace it with:

ftp://ftpgate01.mydomain.com/appserv/support/fixpacks/was61/cumulative/

6.2 Adding files to the repository manually

To use the CIM download function the deployment manager must have access to the public IBM Web sites. When the deployment manager workstation does not have Internet access, you must first download the descriptors and files to a separate workstation that has Internet access, and then manually transfer those files to the centralized installation manager repository.

Alternatively, you can set up an FTP gateway as described in the previous section and perform the download indirectly through the gateway. This section describes how you can add files manually to the repository.

Before you begin

You must first create the centralized installation manager repository on the deployment manager workstation. Complete this task during the installation process of WebSphere Application Server Network Deployment Version 7.0. For more information, see Adding installation package as part of the installation flow.

Alternatively, you can use Installation Factory to add one or more product components to the repository. See Using the Installation Factory to add installation packages for more information.

About this task

The Update Installer and the maintenance files that are required by the centralized installation manager to remotely install maintenance are the same tool and files that are used to apply maintenance to the deployment manager workstation. Complete the steps to download the Update Installer and maintenance files without using the centralized installation manager.

The repository consists of directories where the installation image for the Update Installer and maintenance files are located.

The following lists the directories, along with the URL to use to download additional descriptors:

UPDI70

This directory holds the `7.0.0.0-WS-UPDI-*.zip` file that contains the installation image for the Update Installer. Copy the `7.0.0.0-WS-UPDI-*.zip` file for the various operating systems that you want in this directory.

WAS70Updates

This directory contains all the interim fixes for WebSphere Application Server Network Deployment Version 7.0. Copy the `.pak` files for all your WebSphere Application Server Network Deployment Version 7.0 interim fixes to this directory. You can also remove any `.pak` files that you no longer need from this directory.

WAS70FP*n*

This directory contains various `.pak` files that make up a specific fix pack for WebSphere Application Server. For example, for WebSphere Application Server Network Deployment Version 7.0 Fix Pack 1, copy the `.pak` files to the WAS70FP1 directory. Refer to the WebSphere Application Server Version 7.0 support Web site for the list of files required for each fix pack.

ND61Updates

This directory contains all the interim fixes for WebSphere Application Server Network Deployment Version 6.1. Copy the `.pak` files for all your WebSphere Application Server Network Deployment Version 6.1 interim fixes to this directory. You can also remove any `.pak` files that you no longer need from this directory.

ND61FP*n*

This directory contains the `.pak` files that make up a specific fix pack for WebSphere Application Server. Refer to the WebSphere Application Server Version 6.1 support Web site for the list of files required for each fix pack.

For example, for WebSphere Application Server Network Deployment Version 6.1 Fix Pack 15, copy the following `.pak` files into the ND61FP15 directory:

- `6.1.0-WS-WAS-WinX32-FP0000015.pak`
- `6.1.0-WS-WASSDK-WinX32-FP0000015.pak`
- `6.1.0-WS-WASWebSvc-WinX32-FP0000015.pak`
- `6.1.0-WS-WASEJB3-WinX32-FP0000015.pak`

Add the required files to the centralized installation manager repository to later install recommended fix packs or refresh packs to specific installation targets. Download the descriptors and files to a separate workstation that has Internet access, and then manually transfer those files to the centralized installation manager repository.

Procedure

1. In the administrative console, click **System administration > Centralized Installation Manager > Installation Packages**. Click **Add Packages**, and the Download Descriptors panel is then displayed.

2. Determine the location of the FTP site from which you download the descriptors. Expand the **Download Options** to view the FTP URL that is used by the centralized installation manager. The URL format is `ftp://ftp.software.ibm.com/software/websphere/appserv/support/cim/cim70_yyyymmdd`.

   If the deployment manager workstation does not have Internet access, an error message is displayed indicating that the host name, ftp.software.ibm.com, is not known.

3. Use the URL from the previous step to download the available descriptors from a separate workstation that has Internet access.

4. Transfer the downloaded descriptors to the `<CIM_REPOSITORY_ROOT>/descriptors` directory on the deployment manager workstation.

Results

The centralized installation manager repository now contains maintenance files to install later on the remote workstations.

7 Managing installation targets

You can add or remove an installation target, which is the workstation on which selected software packages might be installed. You can also edit the configuration of an existing installation target, and store the administrative ID and password of each target for later use when installing or uninstalling packages.

Before you begin

You must first create an installation target to install one or more software packages on your workstations. By default, all of the workstations containing nodes that are defined in the cell are displayed as installation targets.

About this task

From the **Installation Targets** page in the administrative console, you can add additional installation targets that are located outside of the cell. For example, you can install the middleware agent on a node that is running other middleware servers that were created outside of the product cell by adding the remote workstation as a new installation target. Other tasks that you can complete to further manage your installation targets include removing installation targets, editing the configuration of installation targets, and installing a Secure Shell (SSH) public key on installation targets. To access this page, click **System administration > Centralized Installation Manager > Installation targets**.

Procedure

- To add additional installation targets that are located outside of the cell, click **Add Installation Target**. The configuration page is displayed next.

    1. Provide the host name and platform of the installation target, and optionally specify the administrative ID and password, which the centralized installation manager later uses to install one or more packages on the installation target.

       Do not use the browser to save the user name and password. The browser might offer the same user name and password on different target names.

    2. Optional: Click **Test Connection** to test the connection using the administrative ID and password that you provide.

    3. Click **OK** after you specify the configuration settings to return to the **Installation targets** page. The new installation target is now displayed in the table.

- To remove existing installation targets, select one or more targets from the table, and click **Remove Installation Target**. The confirmation page then lists each selected installation target. Click **Remove** to complete the action, and to return to the **Installation targets** page.

- To edit the configuration settings of an existing installation target, click the host name. The configuration page is displayed next.

  Edit any of the configuration settings that are displayed on the page, which are the same fields that you complete to configure a newly created installation target.

  Click **OK** after you complete your changes to return to the **Installation targets** page. Any changes that you make now display in the table.

- To install a Secure Shell (SSH) public key on specific installation targets, select one or more targets from the table, and click **Install SSH Public Key**.

  As a result, the wizard is then launched to complete the SSH public key installation process. The actual wizard steps are further explained in Installing the Secure Shell public key to access your remote workstations. Refer to this task for the detailed wizard instructions, and for more information on accessing your remote workstations by using the SSH public/private key pair authentication method.

What to do next

You can now begin installing packages to specific installation targets. For more information on the different types of available installation packages, read a description about each in the detailed instructions for installing packages.

7.1 Installing a Secure Shell public key to access remote workstations

To use Secure Shell (SSH) public/private key as an authentication method for accessing your remote workstations, you must first install the public key of a public/private key pair on the installation targets. You can then securely connect to the remote workstation by using the corresponding private key. Use this topic to install the SSH public key on one or more installation targets.

Before you begin

Linux AIX HP-UX Solaris To successfully complete this task, you must have SSH installed and enabled on the installation target. First create a pair of keys, and install the public key on all the installation targets. Issue the following command to ensure that SSH is started on the workstation:

```
ps -e | grep sshd
```

You can generate an RSA private key and its corresponding public key using the ssh-keygen UNIX command in the following example:

```
ssh-keygen –t rsa
```

Take the default location for storing the private key and make note of it. If you specify a non-empty string for the passphrase prompt, make sure you remember the string because you will need it when you want to use the generated private key.

Additionally, you must know the location of the SSH public key file on the deployment manager, and the administrative ID and password for the installation target. This is the same administrative ID and password that you use to later install or uninstall software packages on the same installation target.

About this task

UNIX and Linux platforms generally support the use of SSH protocol. For Windows operating systems, however, you might have to install third-party software to use SSH protocol. See Using the Secure Shell authentication method on target Windows operating systems for more information.

With the centralized installation manager, you can install product packages and maintenance for distributed platforms directly from the administrative console. Complete the steps that are outlined in the wizard to install the SSH public key, which uses the SSH protocol to communicate with the installation targets.

Procedure

1. To access the wizard from the administrative console, click **System administration > Centralized Installation Manager > Installation targets**.

2. Select one or more existing installation targets from the table, and click **Install SSH Public Key**.

3. Select the appropriate password settings, and click **Next**. You can either select to specify the same user name and password to access all of the installation targets, or you can configure individual user names and passwords for each installation target.

4. Specify the location of the SSH public key file on the deployment manager, and click **Next**.

5. Review the summary of your selections, and click **Finish** to complete the installation process. Click **Previous** to change any of your selections.

Results

You successfully installed the SSH public key on specific installation targets.

What to do next

You can install the same SSH public key on other installation targets to securely access all of your workstations.

7.2 Using the Secure Shell authentication method on target Windows operating systems

For hosts running on Windows operating systems, support for SSH protocol requires the addition of a third-party product such as SSH on CYGWIN on the target Windows host and the software package you are installing will be installed under CYGWIN.

Since WebSphere Application Server does not officially support installing under CYGWIN, this tool has only been tested to verify that CIM can be used to install a software package on Windows targets using the SSH public/private key authentication. Other SSH support for Windows operating systems has not been tested and is not supported by CIM.

Limitation: When installing WebSphere Application Server Version 7.0 on Windows targets using SSH public/private key authentication, do not specify installation directory path with one or more spaces within the path. Having spaces within the installation path will cause failure in some Windows bat file when the input argument also contains spaces.

Before you begin

Use the information provided in this topic only if you want to use the SSH public/private key authentication method to access remote target workstations that are running any of the Windows operating systems. You can skip this topic if you plan to use the user name and password authentication method to access the installation targets.

Ensure CYGWIN SSH server is installed on the Windows target workstation.

In a typical setup of the CYGWIN sshd server running as a Windows service, the server runs under the `Local SYSTEM` account, or for a Windows 2003 Server, runs under a local account, `sshd_server`, specifically created with special privileges to run the service. With an SSH server configured and started on the Windows target, the server authenticates user logins using a public/private key-pair. However, with this setup, installation programs that are located on the Windows target and invoked by the centralized installation manager, which is using public SSH public/private key authentication to gain access to the target workstation, are run using the identity of the account under which the SSH server is running. This causes problems with certain centralized installation manager operations when the files or directories on the target system, which the operation is to operate on, were created using different identities. To work around this, change the service that the CYGWIN sshd server runs under to log on with the same account, `root`, which is used to install software on that specific target Windows workstation.

Assuming that a local ID `root` that has Administrator authority to install software on the Windows workstation has been created, complete the following steps to change the CYGWIN sshd server to run under the ID `root`:

Procedure

1. Change the login ID of the CYGWIN sshd service.

    a. From the Windows Start menu, click **Settings > Control Panel > Administrative Tools > Services**.

    b. From the Services window, right-click **CYGWIN sshd**, and select **Properties**.

    c. From the Properties window, select the **General** tab, and click **Stop** to stop the sshd service.

    d. Next, select the **Log on** tab. Under the **Log on as** section or prompt, clear the **Local System account** radio button, and select **This account**.

    e. Type `.\root` as the ID and type the password for the account. Click **Apply**.

2. Grant additional rights to the `root` account. Ensure that the account has the required privileges in addition to membership to the Administrators group.

    a. From the Windows Start menu, click **Settings > Control Panel > Administrative Tools > Local Security Policy**.

    b. From the Local Security Settings window, expand **Local Policies**, and select **User Rights Assignment**.

c. From the resulting page that is displayed on the right, verify that the `root` account has the following four rights:

   - Adjust memory quotas for a process
   - Create a token object
   - Log on as a service
   - Replace a process level token

   If not, add `root` as a user with the four rights.

   For Windows 2000, the first item in the preceding list is displayed as `Increase quotas` instead of `Adjust memory quotas for a process`.

d. Close the **Local Security Settings** window.

3. From a CYGWIN console panel, change ownership of the following directories and files to `root`:

   - `chown root /var/log/sshd.log`
   - `chown -R root /var/empty`
   - `chown root /etc/ssh*`

4. Restart the CYGWIN sshd service:

   From the **Properties** page of the CYGWIN sshd service, select the **General** tab, and click **Start**. Verify that the service is now running under the `root` user account.

What to do next

You can now install product packages and maintenance to your Windows target workstations. From the administrative console, click **System administration > Centralized Installation Manager > Installation targets**.

8 Conclusion

Centralized installation manager can help to simplify the task of installing and maintaining WebSphere product code in a Network Deployment cell that has multiple nodes. Special considerations when using centralized installation manager to install maintenance are also mentioned.

Section 3 describes typical usage scenarios to help explain how CIM can simplify the tasks of installing and maintaining WebSphere Application Server in a Network Deployment configuration.

CIM also provides a download function to make it easy for the administrator to download maintenance from the IBM Support FTP server directly to the CIM repository. For situations where the deployment manager node does not have direct Internet access to the IBM Support FTP server, a solution involving the set up of an FTP gateway is suggested.

Appendices

Appendix A: Centralized installation manager AdminTask commands

You can use the Jacl or Jython scripting languages to use the features of the centralized installation manager with the wsadmin tool. Use the commands and parameters to install, uninstall, and manage various software packages and maintenance files.

The administrative tasks for the centralized installation manager include the following commands:

- installWASExtension
- installSoftware
- installWithResponseFile
- installMaintenance
- listPackagesForInstall
- listFeaturesForInstall
- showPackageInfo
- showLicenseAgreement
- getManagedNodesOnHostByInstallLoc
- listManagedNodesOnHost
- testConnectionToHost
- testConnectionToHostUsingSSHKey
- installSSHPublicKeyOnHost
- listKeyInstallationRecords
- updateKeyInstallationRecords
- listPendingRequests
- listInProgressRequests
- listRequestsForTarget
- showLatestInstallStatus
- showLatestUninstallStatus
- uninstallSoftware
- uninstallMaintenance

Attention: Several of the commands include an adminName parameter. This refers to the name of an administrator account on the remote target machine. For UNIX targets, this administrator account can be either the root account or a non-root account if the software package supports a non-root install. However, for Windows targets the added requirement is that the user account must have administrative privileges in order to use CIM for remote installations. (See also Appendix B, Question 3.)

installWASExtension

The **installWASExtension** command installs the specified WebSphere® Application Server extension package on a specified host that contains one or more WebSphere Application Server Network Deployment nodes. The nodes must be defined and part of the WebSphere Application Server Network Deployment cell.

Note: This command is applicable if you have installed WebSphere Virtual Enterprise on your deployment manager node.

Target object

None.

Required parameters

-packageName

Specifies the name of the software package. (String, required)

-hostName

Specifies the name of the remote host. (String, required)

-augment

Specifies a list of nodes to augment. Valid nodes are those defined on the host under the same installation location for WebSphere Application Server. Specify ALL_NODES as the keyword value to augment all of the nodes defined for the same installation location. (String, required)

-adminName

Specifies the administrative ID for the remote host. (String, required)

-acceptLicense

Specifies if the license agreement is accepted. Specify true to indicate that you reviewed and agreed to the terms of the IBM® International Program License Agreement accompanying this program. Otherwise, you cannot proceed with the installation of the program or component. (String, required)

Optional parameters

-installLocation

Specifies the path of the installation directory on the remote host. Specify this parameter only if there are multiple installation locations that exist within the current cell on the same host. (String, optional)

-featureList

Specifies a list of features to install on the remote target. (String, optional)

-adminPassword

Specifies the administrative password for the remote host. Specify either the adminPassword command or the privateKeyStore command to authenticate. (String, optional)

-privateKeyStore

Specifies the path to the private key file, which is located on the deployment manager. Specify either the adminPassword command or the privateKeyStore command to authenticate. (String, optional)

-keyStorePassword

Specifies an optional password, also known as the passphrase, which is used to protect the private key file. (String, the parameter is required if a non-blank password is used to protect private key store.)

-specialParms

Specifies optional name-value pairs for other parameters that might be required. Obtain information about any name-value pairs from the provider of the software package. You can also use the showPackageInfo command to gather this information. (String, optional)

-tempDir

Specifies the location of the temporary directory on the target host. If this parameter is omitted, the centralized installation manager uses the default temporary directory of the target host. (String, optional)

Batch mode example usage

- Using Jacl:

```
$AdminTask installWASExtension {-packageName XDOps -hostName river.com
          -augment ALL_NODES -adminName admin1
          -adminPassword  passw0rd1 -acceptLicense true}
```

- Using Jython:

```
AdminTask.installWASExtension ('[-packageName XDOps -hostName river.com
          -augment ALL_NODES -adminName admin1
          -adminPassword passw0rd1 -acceptLicense true]')
```

Interactive mode example usage

- Using Jacl:

```
$AdminTask installWASExtension {-interactive}
```

- Using Jython:

```
AdminTask.installWASExtension ('[-interactive]')
```

installSoftware

The **installSoftware** command installs the specified software package on the target host.

Use this command to install WebSphere Application Server Network Deployment Version 7.0, packageName **ND70**, on remote workstations.

Target object

None.

Required parameters

-packageName

Specifies the name of the software package. (String, required)

-hostName

Specifies the name of the remote host. (String, required)

-platformType

Specifies the operating system of the remote workstation. The valid types are: Windows®, AIX®, HP-UX, Linux®, UNIX®, OS400 or Solaris. This parameter is not case-sensitive. (String, required)

-installLocation

Specifies the path to the installation directory on the remote host. Specify this parameter only if there are multiple installation locations that exist within the current cell on the same host. (String, required)

-adminName

Specifies the administrative ID for the remote host. (String, required)

-acceptLicense

Specifies if the license agreement is accepted. Specify true to indicate that you reviewed and agreed to the terms of the IBM International Program License Agreement accompanying this program. Otherwise, you cannot proceed with the installation of the program or component. (String, required)

Optional parameters

-featureList

Specifies a list of features to install on the remote target. (String, optional)
For the package ND70, available features are:

- **noFeature**, for no feature
- **samplesSelected**, for Application Server samples
- **languagepack.console.all**, for language pack for administrative console
- **languagepack.server.all**, for language pack for server runtime

The default features for this package are: **languagepack.console.all** and **languagepack.server.all**

-adminPassword

Specifies the administrative password for the remote host. Specify either the adminPassword parameter or the privateKeyStore parameter to authenticate. (String, optional)

-privateKeyStore

Specifies the path to the private key file, which is located on the deployment manager. Specify either adminPassword parameter or the privateKeyStore parameter to authenticate. (String, optional)

-keyStorePassword

Specifies an optional password, also known as the passphrase, which is used to protect the private key file. (String, the parameter is required if a non-blank password is used to protect private key store.)

-specialParms

Specifies optional name-value pairs for other parameters that might be required. Obtain information about any name-value pairs from the provider of the software package. You can also use the showPackageInfo command to gather this information. (String, optional)

If global security is enabled for the Network Deployment cell, you must include the following parameters as specialParms:

- DMGR_ADMIN_ID: Specify the administrator ID used to log in to the administrative console.
- DMGR_ADMIN_PWD: Specify the password for the administrator ID used to log in to the administrative console.

Optionally, you can specify the following parameters with the specialParms parameter when you install WebSphere Application Server Network Deployment Version 7.0:

- DISABLE_OS_PREREQ_CHECKING: Specify true or false with this parameter to disable or enable prerequisite checking on the operating system.
- USE_32BIT_IMAGE_ON_64BIT_OS: Specify true if you want to override the default behavior of using 64-bit installation image on 64-bit operating systems. This parameter has effect only if the software package includes a 32-bit image for the platform and machine architecture.

-tempDir

Specifies the location of the temporary directory on the target host. If this parameter is omitted, the centralized installation manager uses the default temporary directory of the target host. (String, optional)

Batch mode example usage

- Using Jacl:

```
$AdminTask installSoftware {-packageName ND70 -hostName abc.com
-platformType windows -installLocation C:/WAS70 -adminName admin1
-adminPassword passw0rd1
-specialParms "{DMGR_ADMIN_ID admin2}{DMGR_ADMIN_PWD passw0rd2}"
-acceptLicense true}
```

```
$AdminTask installSoftware {-packageName ND70 -hostName abc.com
-platformType linux -installLocation "/opt/IBM/WAS70"
-adminName root -adminPassword passw0rd1 -acceptLicense true
-specialParms
"{DISABLE_OS_PREREQ_CHECKING true}{USE_32BIT_IMAGE_ON_64BIT_OS true}"}
```

- Using Jython:

```
AdminTask.installSoftware ('[-packageName ND70 -hostName abc.com
-platformType windows -installLocation C:/WAS70 -adminName admin1
-adminPassword passw0rd1
-specialParms "[DMGR_ADMIN_ID admin2][DMGR_ADMIN_PWD passw0rd2]"
-acceptLicense true]')
```

```
AdminTask.installSoftware ('[-packageName ND70
-featureList noFeature -hostName abc.com
-platformType linux -installLocation "/opt/IBM/WAS70" -adminName admin1
-adminPassword passw0rd1 -acceptLicense true -specialParms
"[DISABLE_OS_PREREQ_CHECKING true]" ]')
```

Interactive mode example usage

- Using Jacl:

```
$AdminTask installSoftware {-interactive}
```

- Using Jython:

```
AdminTask.installSoftware ('[-interactive]')
```

installWithResponseFile

The **installWithResponseFile** command installs the specified software package on the target host using parameters specified in a response file.

Target object

None.

Required parameters

-packageName

Specifies the name of the software package. (String, required)

-hostName

Specifies the domain-qualified host name of the remote host. (String, required)

-platformType

Specifies the operating system of the remote workstation. The valid types are: Windows, AIX, HP-UX, Linux, UNIX, OS400 or Solaris. This parameter is not case-sensitive. (String, required)

-responseFile

Specifies the relative path name of the response file on the deployment manager host that contains the parameters to be used for the installation operation. The response files for centralized installation are kept in the `cim/responsefiles` directory under the deployment manager profile root. The relative pathname is the pathname relative to this directory. (String, required)

-adminName

Specifies the administrative ID for the remote host. (String, required)

-acceptLicense

Specifies whether the terms of the license agreement are accepted. Specify `true` to indicate that you have reviewed and agreed to the terms of the IBM International Program License Agreement accompanying this program. Otherwise, you cannot proceed with the installation of the program or component. (String, required)

Optional parameters

-adminPassword

Specifies the login password of an administrator of the remote host. Either the adminPassword parameter or the privateKeyStore parameter must be specified for authentication. (String, optional)

-privateKeyStore

Specifies the absolute path to the private key file on the deployment manager host. Either the privateKeyStore parameter or the adminPassword parameter must be specified for authentication. (String, optional)

-keyStorePassword

Specifies an optional password, also known as the passphrase, which is used to protect the private key file. (String. The parameter is required if a non-blank password is used to protect the private key store.)

-specialParms

Specifies optional name-value pairs for other parameters that might be required. Obtain information on any required name-value pairs from the provider of the software package. (String, optional)

-tempDir

Specifies the directory path on the target host which the centralized installation manager can use as temporary work space. If this parameter is omitted, the centralized installation manager uses the default temporary directory of the target host. (String, optional)

Batch mode example usage

- Using Jacl:

```
$AdminTask installWithResponseFile {-packageName ND70 -hostName abc.com
-platformType windows –responseFile myOptionsfileForWindows.txt
-adminName admin1 -adminPassword passw0rd1 -acceptLicense true}

$AdminTask installWithResponseFile {-packageName ND70 -hostName
abc.com -platformType aix –responseFile myOptionsfileForAIX.txt
-adminName root -adminPassword passw0rd1 -acceptLicense true
-specialParms "{USE_32BIT_IMAGE_ON_64BIT_OS true}"}
```

- Using Jython:

```
AdminTask.installWithResponseFile ('[-packageName ND70 -hostName
abc.com -platformType linux –responseFile myOptionsfileForLinux.txt
-adminName root -adminPassword passw0rd1 -acceptLicense true]')

AdminTask.installWithResponseFile ('[-packageName ND70 -hostName
abc.com -platformType aix –responseFile myOptionsfileForAIX.txt
-adminName root -adminPassword passw0rd1 -acceptLicense true
-specialParms "[USE_32BIT_IMAGE_ON_64BIT_OS true]"]')
```

Interactive mode example usage

- Using Jacl:

```
$AdminTask installWithResponseFile {-interactive}
```

- Using Jython:

```
AdminTask.installWithResponseFile ('[-interactive]')
```

installMaintenance

The **installMaintenance** command installs maintenance on the target host.

Target object

None.

Required parameters

-packageName

Specifies the name of the software package. (String, required)

-hostName

Specifies the name of the remote host. (String, required)

-adminName

Specifies the administrative ID for the remote host. (String, required)

-acceptLicense

Specifies if the license agreement is accepted. Specify true to indicate that you reviewed and agreed to the terms of the IBM International Program License Agreement accompanying this program. Otherwise, you cannot proceed with the installation of the program or component. (String, required)

Optional parameters

-fileList

Specifies a list of .pak maintenance files to install on the remote target. This parameter is ignored if you install a predefined maintenance package. (String, optional)

-installLocation

Specifies the path of the installation directory in which to install the package on the remote host. Specify this parameter only if there are multiple installation locations that exist within the current cell on the same host. (String, optional)

-adminPassword

Specifies the administrative password for the remote host. Specify either the adminPassword parameter or the privateKeyStore parameter to authenticate. (String, optional)

-privateKeyStore

Specifies the path to the private key file, which is located on the deployment manager. Specify either adminPassword parameter or the privateKeyStore parameter to authenticate. (String, optional)

-keyStorePassword

Specifies an optional password, also known as the passphrase, which is used to protect the private key file. (String, the parameter is required if a non-blank password is used to protect private key store.)

-tempDir

Specifies the location of the temporary directory on the target host. If this parameter is omitted, the centralized installation manager uses the default temporary directory of the target host. (String, optional)

Batch mode example usage

- Using Jacl:

```
$AdminTask installMaintenance {-packageName ND61Maintenance -fileList
"6.1.0.9-WS-WAS-IFPKxxxxx.pak,6.1.0.9-WS-WAS-IFPKyyyyy.pak" -hostName
river.com -installLocation D:/WAS61 -adminName admin1 -adminPassword
passw0rd1 -acceptLicense true}
```

- Using Jython:

```
AdminTask.installMaintenance ('[-packageName ND61Maintenance -fileList
"6.1.0.9-WS-WAS-IFPKxxxxx.pak,6.1.0.9-WS-WAS-IFPKyyyyy.pak" -hostName
river.com -installLocation D:/WAS61 -adminName admin1 -adminPassword
passw0rd1 -acceptLicense true]')
```

Interactive mode example usage

- Using Jacl:

```
$AdminTask installMaintenance {-interactive}
```

- Using Jython:

```
AdminTask.installMaintenance ('[-interactive]')
```

listPackagesForInstall

The **listPackagesForInstall** command lists all of the software packages that you can use the centralized installation manager to install.

Target object

None.

Required parameters

None.

Optional parameters

None.

Batch mode example usage

- Using Jacl:

  ```
  $AdminTask listPackagesForInstall
  ```

- Using Jython:

  ```
  AdminTask.listPackagesForInstall ()
  ```

Interactive mode example usage

- Using Jacl:

  ```
  $AdminTask listPackagesForInstall {-interactive}
  ```

- Using Jython:

  ```
  AdminTask.listPackagesForInstall ('[-interactive]')
  ```

listFeaturesForInstall

The **listFeaturesForInstall** command lists the available features of a software package that you can use the centralized installation manager to install.

None of the WebSphere Virtual Enterprise components provide separately installable features. This command returns an empty list when used against one of the WebSphere Virtual Enterprise components.

Target object

None.

Required parameters

-packageName

Specifies the name of the software package. (String, required)

Optional parameters

None.

Batch mode example usage

- Using Jacl:

```
$AdminTask listFeaturesForInstall {-packageName sample_package}
```

- Using Jython:

```
AdminTask.listFeaturesForInstall ('[-packageName sample_package]')
```

Interactive mode example usage

- Using Jacl:

```
$AdminTask listFeaturesForInstall {-interactive}
```

- Using Jython:

```
AdminTask.listFeaturesForInstall ('[-interactive]')
```

showPackageInfo

The **showPackageInfo** command displays general information about a specific software package.

Target object

None.

Required parameters

-packageName

Specifies the name of the software package. (String, required)

Optional parameters

None.

Batch mode example usage

- Using Jacl:

```
$AdminTask showPackageInfo {-packageName sample_package}
```

- Using Jython:

```
AdminTask.showPackageInfo ('[-packageName sample_package]')
```

Interactive mode example usage

- Using Jacl:

```
$AdminTask showPackageInfo {-interactive}
```

- Using Jython:

```
AdminTask.showPackageInfo ('[-interactive]')
```

showLicenseAgreement

The **showLicenseAgreement** command displays the license agreement associated with the specified installation package.

Target object

None.

Required parameters

-packageName

Specifies the name of the software package. (String, required)

Optional parameters

-showLicenseInfoOnly

Specifies that only the content of the license file is shown. The default is false. (String, required)

Batch mode example usage

- Using Jacl:

  ```
  $AdminTask showLicenseAgreement {-packageName sample_package}
  ```

- Using Jython:

  ```
  AdminTask.showLicenseAgreement ('[-packageName sample_package]')
  ```

Interactive mode example usage

- Using Jacl:

  ```
  $AdminTask showLicenseAgreement {-interactive}
  ```

- Using Jython:

  ```
  AdminTask.showLicenseAgreement ('[-interactive]')
  ```

getManagedNodesOnHostByInstallLoc

The **getManagedNodesOnHostByInstallLoc** command returns the names of the managed nodes that are defined in the current deployment manager cell. Issue this command when a host contains multiple installations of WebSphere Application Server Network Deployment with nodes that are federated into the same cell.

Target object

The required target object is the host name of the workstation containing the managed nodes that are federated into the current deployment manager cell.

Required parameters

None.

Optional parameters

None.

Batch mode example usage

- Using Jacl:

  ```
  $AdminTask getManagedNodesOnHostByInstallLoc host_name
  ```

- Using Jython:

  ```
  AdminTask.getManagedNodesOnHostByInstallLoc ('host_name')
  ```

Interactive mode example usage

- Using Jacl:

  ```
  $AdminTask getManagedNodesOnHostByInstallLoc {-interactive}
  ```

- Using Jython:

  ```
  AdminTask.getManagedNodesOnHostByInstallLoc ('[-interactive]')
  ```

listManagedNodesOnHost

The **listManagedNodesOnHost** command lists the managed nodes that are located on the federated host in the current deployment manager cell.

Target object

The required target object specifies the host name of the workstation containing the managed nodes that are federated into the deployment manager cell.

Required parameters

None.

Optional parameters

None.

Batch mode example usage

- Using Jacl:

  ```
  $AdminTask listManagedNodesOnHost host_name
  ```

- Using Jython:

  ```
  AdminTask.listManagedNodesOnHost ('host_name')
  ```

Interactive mode example usage

- Using Jacl:

  ```
  $AdminTask listManagedNodesOnHost {-interactive}
  ```

- Using Jython:

  ```
  AdminTask.listManagedNodesOnHost ('[-interactive]')
  ```

testConnectionToHost

The **testConnectionToHost** command verifies that a connection can be established from the deployment manager to the remote host by using an administrator ID and password for the remote host.

Target object

None.

Required parameters

-hostName

Specifies the name of the remote host. (String, required)

-platformType

Specifies the platform type of the remote host. The valid types are Windows, AIX, HP-UX, Linux, UNIX, OS400 or Solaris. This parameter is not case-sensitive. (String, required)

-adminName

Specifies the administrative ID for the remote host. (String, required)

-adminPassword

Specifies the administrative password for the remote host. (String, required)

Optional parameters

None.

Batch mode example usage

- Using Jacl:

```
$AdminTask testConnectionToHost {-hostName big.mountain.com
-platformType linux -adminName root -adminPassword passw0rd3}
```

- Using Jython:

```
AdminTask.testConnectionToHost ('[-hostName big.mountain.com
-platformType linux -adminName root -adminPassword passw0rd3]')
```

Interactive mode example usage

- Using Jacl:

```
$AdminTask testConnectionToHost {-interactive}
```

- Using Jython:

```
AdminTask.testConnectionToHost ('[-interactive]')
```

testConnectionToHostUsingSSHKey

The **testConnectionToHostUsingSSHKey** command verifies that a connection can be established from the deployment manager to the remote host by using the Secure Shell (SSH) private key for the remote host.

Target object

None.

Required parameters

-hostName

Specifies the name of the remote host. (String, required)

-adminName

Specifies the administrative ID for the remote host. (String, required)

-privateKeyStore

Specifies the path to the private key file, which is located on the deployment manager. (String, required)

Optional parameters

-keyStorePassword

Specifies the optional password, also known as the passphrase, which is used to protect the private key file. (String, the parameter is required if a non-blank password is used to protect private key store.)

Batch mode example usage

- Using Jacl:

```
$AdminTask testConnectionToHostUsingSSHKey {-hostName abc.com
-adminName root -privateKeyStore /root/.ssh/id_rsa}
```

- Using Jython:

```
AdminTask.testConnectionToHostUsingSSHKey ('[-hostName abc.com
-adminName root -privateKeyStore /root/.ssh/id_rsa]')
```

Interactive mode example usage

- Using Jacl:

```
$AdminTask testConnectionToHostUsingSSHKey {-interactive}
```

- Using Jython:

```
AdminTask.testConnectionToHostUsingSSHKey ('[-interactive]')
```

installSSHPublicKeyOnHost

The **installSSHPublicKeyOnHost** command installs the administrative Secure Shell (SSH) public key on the remote host.

Target object

None.

Required parameters

-hostName

Specifies the name of the remote host. (String, required)

-adminName

Specifies the administrative ID for the remote host. (String, required)

-adminPassword

Specifies the administrative password for the remote host. (String, required)

-publicKeyStore

Specifies the path to the public key file, which is located on the deployment manager, in either Internet Engineering Task Force (IETF) standard format or OpenSSH format.

Optional parameters

None.

Batch mode example usage

- Using Jacl:

```
$AdminTask installSSHPublicKeyOnHost {-hostName abc.com -adminName root
-adminPassword passw0rd3 -publicKeyStore /root/.ssh/id_rsa.pub}
```

- Using Jython:

```
AdminTask.installSSHPublicKeyOnHost ('[-hostName abc.com -adminName
root -adminPassword passw0rd3 -publicKeyStore /root/.ssh/id_rsa.pub]')
```

Interactive mode example usage

- Using Jacl:

```
$AdminTask installSSHPublicKeyOnHost {-interactive}
```

- Using Jython:

```
AdminTask.installSSHPublicKeyOnHost ('[-interactive]')
```

listKeyInstallationRecords

The **listKeyInstallationRecords** command lists the SSH public key installation records that the centralized installation manager maintains.

Target object

None.

Required parameters

None.

Optional parameters

None.

Batch mode example usage

- Using Jacl:

```
$AdminTask listKeyInstallationRecords
```

- Using Jython:

```
AdminTask.listKeyInstallationRecords ()
```

Interactive mode example usage

- Using Jacl:

```
$AdminTask listKeyInstallationRecords {-interactive}
```

- Using Jython:

```
AdminTask.listKeyInstallationRecords ('[-interactive]')
```

updateKeyInstallationRecords

The **updateKeyInstallationRecords** command updates the SSH public key installation records that the centralized installation manager maintains.

Target object

None.

Required parameters

None.

Optional parameters

-add

Adds a list of host names to the installation records. (String, optional)

-remove

Removes a list of host names from the installation records. (String, optional)

Batch mode example usage

- Using Jacl:

  ```
  $AdminTask updateKeyInstallationRecords {-add "abc.com,river.com"}
  ```

- Using Jython:

  ```
  AdminTask.updateKeyInstallationRecords ('[-add "abc.com,river.com"]')
  ```

Interactive mode example usage

- Using Jacl:

  ```
  $AdminTask updateKeyInstallationRecords {-interactive}
  ```

- Using Jython:

  ```
  AdminTask.updateKeyInstallationRecords ('[-interactive]')
  ```

listPendingRequests

The **listPendingRequests** command lists the submitted installation or uninstallation requests that are not started

Target object

None.

Required parameters

None.

Optional parameters

None.

Batch mode example usage

- Using Jacl:

```
$AdminTask listPendingRequests
```

- Using Jython:

```
AdminTask.listPendingRequests ()
```

Interactive mode example usage

- Using Jacl:

```
$AdminTask listPendingRequests {-interactive}
```

- Using Jython:

```
AdminTask.listPendingRequests ('[-interactive]')
```

listInProgressRequests

The **listInProgressRequests** command lists the installation or uninstallation requests that are in progress for completion.

Target object

None.

Required parameters

None.

Optional parameters

None.

Batch mode example usage

- Using Jacl:

  ```
  $AdminTask listInProgressRequests
  ```

- Using Jython:

  ```
  AdminTask.listInProgressRequests ()
  ```

Interactive mode example usage

- Using Jacl:

  ```
  $AdminTask listInProgressRequests {-interactive}
  ```

- Using Jython:

  ```
  AdminTask.listInProgressRequests ('[-interactive]')
  ```

listRequestsForTarget

The **listRequestsForTarget** command lists all of the submitted installation and uninstallation requests for a specific host.

Target object

The required target object the host name of the target workstation. You must specify the same host name that you use for the **installSoftware** and **uninstallSoftware** commands.

Required parameters

None.

Optional parameters

None.

Batch mode example usage

- Using Jacl:

  ```
  $AdminTask listRequestsForTarget host_name
  ```

- Using Jython:

  ```
  AdminTask.listRequestsForTarget ('host_name')
  ```

Interactive mode example usage

- Using Jacl:

  ```
  $AdminTask listRequestsForTarget {-interactive}
  ```

- Using Jython:

  ```
  AdminTask.listRequestsForTarget ('[-interactive]')
  ```

showLatestInstallStatus

The **showLatestInstallStatus** command lists all of the submitted installation requests for a specific host.

Target object

The required target object is the host name of the target workstation. You must specify the same host name that you use for the **installSoftware** command.

Required parameters

None.

Optional parameters

None.

Batch mode example usage

- Using Jacl:

  ```
  $AdminTask showLatestInstallStatus host_name
  ```

- Using Jython:

  ```
  AdminTask.showLatestInstallStatus ('host_name')
  ```

Interactive mode example usage

- Using Jacl:

  ```
  $AdminTask showLatestInstallStatus {-interactive}
  ```

- Using Jython:

  ```
  AdminTask.showLatestInstallStatus ('[-interactive]')
  ```

showLatestUninstallStatus

The **showLatestUninstallStatus** command displays the status of the most recently submitted uninstallation request.

Target object

The required target object is the host name of the target workstation. You must specify the same host name that you use for the **uninstallSoftware** command.

Required parameters

None.

Optional parameters

None.

Batch mode example usage

- Using Jacl:

  ```
  $AdminTask showLatestUninstallStatus host_name
  ```

- Using Jython:

  ```
  AdminTask.showLatestUninstallStatus ('host_name')
  ```

Interactive mode example usage

- Using Jacl:

  ```
  $AdminTask showLatestUninstallStatus {-interactive}
  ```

- Using Jython:

  ```
  AdminTask.showLatestUninstallStatus ('[-interactive]')
  ```

uninstallSoftware

The **uninstallSoftware** command uninstalls the software package from the remote host.

Target object

None.

Required parameters

-packageName

Specifies the name of the software package. (String, required)

-hostName

Specifies the name of the remote host. (String, required)

-platformType

Specifies the operating system of the remote workstation. The valid types are Windows, AIX, HP-UX, Linux, UNIX, OS400 or Solaris. This parameter is not case-sensitive. (String, required)

-installLocation

Specifies the path to the installation directory on the remote host. Specify this parameter only if there are multiple installation locations that exist within the current cell on the same host. (String, required)

-adminName

Specifies the administrative ID for the remote host. (String, required)

Optional parameters

-adminPassword

Specifies the administrative password for the remote host. Specify either the adminPassword parameter or the privateKeyStore parameter to authenticate. (String, optional)

-privateKeyStore

Specifies the path to the private key file, which is located on the deployment manager. Specify either the adminPassword parameter or the privateKeyStore parameter to authenticate. (String, optional)

-keyStorePassword

Specifies an optional password, also known as the passphrase, which is used to protect the private key file. (String, the parameter is required if a non-blank password is used to protect private key store.)

Batch mode example usage

- Using Jacl:

```
$AdminTask uninstallSoftware {-packageName ND70 -hostName abc.com
-platformType windows -installLocation C:/WAS70 -adminName admin1
-adminPassword passw0rd1}
```

- Using Jython:

```
AdminTask.uninstallSoftware ('[-packageName ND70 -hostName abc.com
-platformType windows -installLocation C:/WAS70 -adminName admin1
-adminPassword passw0rd1]')
```

Interactive mode example usage

- Using Jacl:

```
$AdminTask uninstallSoftware {-interactive}
```

- Using Jython:

```
AdminTask.uninstallSoftware ('[-interactive]')
```

uninstallMaintenance

The **uninstallMaintenance** command uninstalls maintenance, such as fix packs and interim fixes, from the remote host.

Target object

None.

Required parameters

-packageName

Specifies the name of the software package. (String, required)

-hostName

Specifies the name of the remote host. (String, required)

-adminName

Specifies the administrative ID for the remote host. (String, required)

Optional parameters

-fileList

Specifies a list of maintenance files to uninstall on the remote target. (String, optional)

-installLocation

Specifies the path to the installation directory on the remote host. Specify this parameter only if there are multiple installation locations that exist within the current cell on the same host. (String, optional)

-adminPassword

Specifies the administrative password for the remote host. Specify either the adminPassword parameter or the privateKeyStore parameter to authenticate. (String, optional)

-privateKeyStore

Specifies the path to the private key file, which is located on the deployment manager. Specify either the adminPassword parameter or the privateKeyStore parameter to authenticate. (String, optional)

-keyStorePassword

Specifies an optional password, also known as the passphrase, which is used to protect the private key file. (String, the parameter is required if a non-blank password is used to protect private key store.)

Batch mode example usage

- Using Jacl:

```
$AdminTask uninstallMaintenance {-packageName ND61Maintenance -hostName
river.com -adminName admin1 -adminPassword passw0rd1 -fileList
"6.1.0.9-WS-WAS-IFPKxxxxx.pak,6.1.0.9-WS-WAS-IFPKyyyyy.pak"}
```

- Using Jython:

```
AdminTask.uninstallMaintenance ('[-packageName ND61Maintenance
-hostName river.com -adminName admin1 -adminPassword passw0rd1
-fileList "6.1.0.9-WS-WAS-IFPKxxxxx.pak,
6.1.0.9-WS-WAS-IFPKyyyyy.pak"]')
```

Interactive mode example usage

- Using Jacl:

```
$AdminTask uninstallMaintenance {-interactive}
```

- Using Jython:

```
AdminTask.uninstallMaintenance ('[-interactive]')
```

Appendix B: Troubleshooting installations

Question 1: I was trying to use CIM to install an interim fix for the Feature Pack for Web Services on a WebSphere Application Server 6.1 host that I have in my Version 7.0 Network Deployment cell. However, the CIM Available installations panel, Show Installation Targets function does not list my host as an available installation target. Why?

Answer: WebSphere Application Server Version 6.1 Feature Pack installations without a profile created for the environment is not visible to CIM as an installed product on the target host. To make the deployment manager and CIM aware that the Version 6.1 Feature Pack is installed, you have to create a Feature Pack for Web Services profile and federate the defined node to the deployment manager. For feature packs installed on Version 7.0 application server hosts this is not necessary because CIM has added support to handle this situation.

Question 2: My deployment manager is on a Windows workstation and I have generated a public-private key pair to use SSH authentication with remote target hosts running on UNIX platforms. But CIM cannot access the private key store on the deployment manager workstation. Why?

Answer: If you had generated a public-private key pair on your Windows workstation using the OpenSSH package that is part of CYGWIN, the private key store is protected and is accessible only to the user account that creates the key pair. However, the default setup for WebSphere Application Server on Windows operating system is to have the server running under the local `SYSTEM` account. To allow CIM to access the private key store you must also grant the local `SYSTEM` account read permission to the private key store:

1. From the Windows Explorer navigate to the private key store, right click the key store file name, `id_rsa`, for example, and select **Properties**.

2. Select the **Security** tab and add the SYSTEM account giving **Read** and **Read & Execute** permissions to the account.

3. Click **OK**.

Question 3: I got the following error trying to connect to my Windows workstation using a non-administrator user ID and password:

```
XCIM0010E: An error occurred while connecting to the remote target
<ip_address>. Cause: CTGRI0011E An error occurred when accessing the remote
registry or service control manager.
```

Answer: Many operations that CIM performs require access to resources that are not generally accessible by ordinary user accounts. Therefore, the account names that you use to log onto remote Windows machines must have administrative privileges. The simplest way is to add the user account to the Administrators group using the following steps:

1. Right click **My Computer** from your Windows desktop and select **Manage**.

2. Expand **Local Users and Groups** on the resulting Computer Management windows and select the **Users** folder.

3. On the right panel, double-click the user account to open the Properties window for that account.

4. Select the **Member Of** tab, and add the **Administrators** group to the list of groups that this account belongs to.

Question 4: I installed WebSphere Application Server Version 7.0 using a response file on a remote host through the centralized installation manager. I did not federate the node to the deployment manager. Later, I tried to use CIM to uninstall the server but the Show Uninstallation Targets function in the CIM Available installations panel does not list my host as an available uninstallation target. Why?

Answer: The centralized installation manager only works on nodes that are part of the deployment manager cell. Since your node is not federated to the cell, you must run the uninstaller locally to uninstall the server.

Appendix C: Notices

References in this publication to IBM products, programs, or services do not imply that IBM intends to make these available in all countries in which IBM operates. Any reference to an IBM product, program, or service is not intended to state or imply that only IBM's product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any of IBM's intellectual property rights may be used instead of the IBM product, program, or service. Evaluation and verification of operation in conjunction with other products, except those expressly designated by IBM, is the user's responsibility.

IBM may have patents or pending patent applications covering subject matter in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to the following address:

IBM Director of Licensing
IBM Corporation
500 Columbus Avenue
Thornwood, New York 10594
USA

Appendix D: Trademarks and service marks

IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both. If these and other IBM trademarked terms are marked on their first occurrence in this information with a trademark symbol (® or ™), these symbols indicate U.S. registered or common law trademarks owned by IBM at the time this information was published. Such trademarks may also be registered or common law trademarks in other countries. A current list of IBM trademarks is available on the Web at Copyright and trademark information at www.ibm.com/legal/copytrade.shtml.

Microsoft and Windows are trademarks of Microsoft Corporation in the United States, other countries, or both.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Java is a trademark of Sun Microsystems, Inc. in the United States, other countries, or both.

Other company, product, or service names may be trademarks or service marks of others.