IBM Maximo Asset Management
Version 7 Release 5

Installation Guide

(WebSphere Application Server, Oracle, Tivoli Directory Server)

Note

Before using this information and the product it supports, read the information in "Notices" on page 213.

This edition applies to version 7, release 5, modification 0 of IBM Maximo Asset Management and to all subsequent releases and modifications until otherwise indicated in new editions.

Contents

Chapter 10. Uninstalling the product 131

Chapter 11. Starting and stopping middleware 143

Chapter 12. Advanced installation topics. 149

Chapter 13. Middleware on Solaris and HP-UX 157

Chapter 14. Backup and restoration 171

Chapter 15. Troubleshooting 185

Chapter 1. Preparing for installation

These topics provide information about product media, preinstallation considerations, overview of the installation procedure, and instructions on using the Maximo® Asset Management launchpad.

Use the planning information to familiarize yourself with the overall process of a Maximo Asset Management deployment before you use this information to conduct the installation.

Software installation images

You access the IBM® Maximo Asset Management product software from IBM Passport Advantage or from the product DVD if you requested a product DVD.

The installation images that you download from Passport Advantage can comprise multiple downloadable files. Download all files in the package to a single directory and extract the files for execution.

For instructions and a full list of installation images, see the IBM Maximo Asset Management 7.5 Download Document (www.ibm.com/support/docview.wss?uid=swg24029458).

Before you begin

A set of tasks must be completed before installing Maximo Asset Management. In some cases, to perform the steps, you must be logged in as a user with administrator privileges on Windows. Some processes, such as anti-virus programs, can negatively affect Maximo Asset Management installation on the system. You must temporarily shut down any noncritical processes before running the Maximo Asset Management installation program.

Most tasks must be completed for middleware installed on UNIX systems, regardless of whether you intend to use the middleware installation program to install and configure Maximo Asset Management middleware. These tasks must be completed for any UNIX systems hosting middleware you intend to use with Maximo Asset Management.

Note: Make a copy of the image of the system, database, and application server on which you are planning to install the product.

Note: IBM publishes updates to the middleware installation program. Before using it, visit the IBM Support Portal http://www.ibm.com/support/entry/portal/Overview/Software/Tivoli/Maximo_Asset_Management to see whether there is an updated copy of the installation program available for your use.

Ensure that you have adequate disk space for the future on the systems being used for the Maximo Asset Management deployment. Filling up the disk space on a Maximo Asset Management deployment system can cause problems with Maximo Asset Management operations.

Fully qualified host names provided to the installation programs must resolve between systems involved in the product deployment. Ensure all IP addresses configured for systems targeted for the product deployment are reachable using the ping command from the administrative workstation.

“Checking port availability” on page 7
You need to ensure that certain ports are available before using the product installation programs.

“AIX and HP-UX tar command requirements” on page 7
Both the native UNIX**tar** command and the GNU version of the **tar** command are required by the middleware installation program. Because the native utility does not support long file names, ensure that GNU **tar** version 1.14 or higher is installed. GNU **tar** version 1.14 ensures that installation files can be extracted.

“Enabling asynchronous I/O on AIX” on page 8
IBM Tivoli® Directory Server requires asynchronous I/O be enabled on AIX® systems.

“Checking for required libraries on Linux” on page 9
The Maximo Asset Management deployment requires certain Linux system libraries.

“Configuring the JRE in Linux” on page 9
In some cases, the middleware installation program fails on Red Hat Enterprise Linux 5 systems, or other systems with Security-Enhanced Linux (SELinux) enabled.

“Setting the ulimit” on page 9
This section details how to set the ulimit in Linux, which is used to define user system and process resource limits.

“Setting the swap size” on page 10
Maximo Asset Management can be a resource-intensive application. Configure and tune your system for maximum performance. This section details how to set the size of the swap space used in Linux systems.

“Setting shared memory” on page 10
This section details how to set a minimum shared memory value in Linux.

“Remote configuration enablement” on page 10
The Maximo Asset Management installation program can automatically configure middleware. You must enable a remote access protocol for each system on which you intend to install the middleware.

“Enabling SSL client authentication” on page 12
The Maximo Asset Management installation program and the process solution installer fail if the client authentication feature of secure sockets layer (SSL) is enabled in the IBM HTTP Server. You can use a workaround to enable client authentication during installation.

“System password policy settings” on page 13
Be familiar with the password policies of systems you are using as part of a Maximo Asset Management deployment.

“Backing up the Deployment Engine database” on page 13
These instructions are for backing up the Deployment Engine database. Backups are used to restore the database to the state it was before installing.

“Programmatically verifying prerequisites” on page 3
You can use the prerequisite verification utility to verify that installation program prerequisites are present on a system. Use this utility before starting the middleware and product installation programs.

Programmatically verifying prerequisites

You can use the prerequisite verification utility to verify that installation program prerequisites are present on a system. Use this utility before starting the middleware and product installation programs.

About this task

The prerequisite verification utility checks the following items:

- Operating system requirements, including fix packs.
- Hardware requirements, including memory and hard disk space.
- Port availability.
- Middleware requirements such as software packages, library files, directory permissions, host names, and installation locations.

You can start the prerequisite verification utility from the product installation launchpad or from the command line. When started from the launchpad, the utility runs in interactive mode. When started from the command line, the prerequisite verification utility accepts various parameters. The prerequisite verification utility must be run on the system hosting the prerequisite being checked. You cannot use this utility to check prerequisites on a remote system.

Table 1. System verification parameters

Parameters	Details
-component	Specifies the type of component being verified. At least one component must be used with the prerequisite verification utility. **dirserver** Use the **dirserver** parameter to have the prerequisite verification utility check for IBM Tivoli Directory Server prerequisites. **j2eeserver** Use the **j2eeserver** parameter to have the prerequisite verification utility check for WebSphere® Application Server Network Deployment prerequisites. **bsi** Use the **bsi** parameter to have the prerequisite verification utility check for prerequisites required by the product installation program. Run the prerequisite verification utility with the **bsi** parameter on the administrative workstation. Syntax example: `tpae_req_check.bat -component bsi` If you do not use the **-component** parameter, you are prompted to specify components when using the utility. Multiple components can be specified as comma-separated values.

Table 1. System verification parameters (continued)

Parameters	Details
-input	The prerequisite verification utility can accept a property file as input. The utility verifies property values found in the file. The default input property file is `tpae.properties`, and is found on the middleware installation media in the `SystemRequirements` directory. There are also several sample property files found in the `SystemRequirements\sample_property_files`. These sample property files contain custom values defined for particular operating systems. You can copy these property files to the system and modify them, or create your own, before running the prerequisite verification utility. Syntax example: `tpae_req_check.bat -component dbserver -input` *`path to the property file`* If you do not use the **input** parameter when you run the prerequisite verification utility, the utility is run in interactive mode. You are prompted for individual values to be verified.

-mode	The prerequisite verification utility can be run in silent or interactive mode.
	interactive
	By default, the prerequisite verification utility is run in interactive mode. If you do not specify the **-mode** parameter, the utility defaults to running in interactive mode. When started from the launchpad, the utility runs in interactive mode.
	silent
	If you use the **silent** qualifier, you can also use the **input** parameter and supply a property file. If an input file not provided, default property values are used. The output must also be directed to a file to view the results.
	Syntax example:
	`tpae_req_check.bat`
	`-component dbserver`
	`-mode silent`
	`-input` *`path to the property file`* `> prereqresults.log`

-lang	Parameter used to specify the locale of the system being verified.
	Syntax example:
	`tpae_req_check.bat`
	`-component dbserver`
	`-lang en`
	Results are produced in the language of the locale specified.
	This is an optional parameter.
	By default, the language set in the system locale is used. If the resource bundle is not found for the system locale, or, the system locale language is not supported, messages are displayed in English.

Table 1. System verification parameters (continued)

Parameters	Details

-trace	Parameter used to specify trace output statements while the utility is running.
	None
	Selecting this qualifier results in no trace information being generated while the utility is running.
	Verbose
	Selecting this qualifier results in detailed trace information being generated while the utility is running.
	Normal
	Selecting this qualifier results in default trace information being generated while the utility is running.
	Syntax example:
	`tpae_req_check.bat`
	`-component dbserver`
	`-trace None`

Procedure

1. Log on to the system you are checking for prerequisites with a user ID that has permission to run scripts on the system. Ensure that the middleware installation media is mounted or otherwise available to the system.
2. Open a command-line window and change directory to the `SystemRequirements` directory of the middleware installation media.
3. Run the prerequisite verification utility. Specify the component being checked and the property file to use.

   ```
   tpae_req_check.bat
   -component dbserver
   -input d:\SystemRequirements\tpae.properties
   ```

   In this example, the `tpae.properties` file is located in the same directory as the `tpae_req_check.bat` script.

Results

After the prerequisite verification utility has completed successfully, results are printed to the screen.

```
CTGIN8117I : The Tivoli Pre-requisite Scanner has been launched.
CTGIN8118I : The Tivoli Pre-requisite Scanner exited with the return code
IBM Prerequisite Scanner
    Version  : 1.0.34
    Build    : 20101109
    OS Name  : Microsoft Windows Server 2003, Enterprise Edition Service Pack 2
    User Name: Administrator

Machine Info
   Machine name : MYMACHINE
   Serial Number: KKKKKK0
   OS Serial    : 66666-666-6666666-66666

PAE [not defined] [version 07500000]:
Property                                Result  Found                                   Exp...
========                                ======  =====                                   ===...
os.totalPhysicalMemory                  PASS    2.00GB                                  1.90GB
network.hasFQDN                         FAIL    False                                   True
Disk#1 (C:\ibm\tivoli\mwi\workspace)    PASS    27.99GB                                 300MB
```

```
Disk#2 (C:\Temp\1)                   PASS    27.99GB                                 1000MB
Disk#3 (C:\Temp\1)                   PASS    27.99GB                                 250MB
network.availablePorts.db2           PASS    135,445,1025,2967,3389,5800,5900,139    50000
network.availablePorts.ctginst       PASS    135,445,1025,2967,3389,5800,5900,139    50005
Disk#4 (C:\Program Files\IBM\SQLLIB)    PASS    27.99GB                              1.40GB

ALL COMPONENTS :
Property           Result     Found     Exp...
========           ======     =====     ===...
C:                 PASS       27.99GB   2.91GB

Prereq Scanner Overall Result: FAIL
prereq_checker.bat 1
```

These values can also be redirected to a file when starting the command from the command line.

If any of the verification steps report a failure, resolve the issue and rerun the verification utility before installing Maximo Asset Management components.

Table 2 contains a list of the properties checked. Use this information to analyze prerequisite verification utility results.

Table 2. Prerequisite verification utility properties

Property	**Description**
CpuArchitecture	Verifies the machine architecture is supported.
disk(rw permissions)	Checks read/write permissions of required directories.
network.availablePorts.*	Verifies required ports are available.
network.dns	Verifies there is a DNS entry for the system on the DNS server.
network.fqdn	Verifies that the system host name is fully qualified.
os.architecture	Verifies the operating system architecture is supported.
os.dir.tmp/home	Verifies required permissions for the system directories
os.FreePagingSpace	Verifies adequate free paging space is available on the system.
os.iodevicestatus	Verifies the I/O device status of the system.
os.lib.ksh	Checks the ksh library.
os.lib.libstdc++.so.5	Verifies a prerequisite library is available on the system.
os.lib.xlC.rte=xlC.rte.9.0.0.8+	Verifies a prerequisite library is available on the system.
os.mountcheck	Checks for the existence of `nosuid` on the file system.
os.package.rpm	Verifies prerequisite packages are available on the system.
os.RAMSize	Reports system RAM available.
os.SELinux	Determines if `selinux` is enabled.
os.servicePack	Verifies required service packs are installed on the system.
os.shell.default	Determines the default shell for users.
os.space.*	Determines disk space availability for various file systems. The following example shows the check made for the middleware installation program workspace. `os.space.root=[dir:root=/root/ibm/tivoli/mwi/workspace,unit:MB]300`
os.totalPhysicalMemory	Reports physical RAM available to the operating system.
os.ulimit	Identifies user limits configured on the system.
os.Version	Reports the operating system type and version.

Checking port availability

You need to ensure that certain ports are available before using the product installation programs.

About this task

You must check to see if ports are in use and accepting connections for the system you are using to host middleware.

Port 9060 must be made available for IBM WebSphere Application Server Network Deployment.

If you intend to use these default port values, ensure that the port is not already assigned before you run installation programs.

You can either use the prerequisite verification utility to check for port availability, or you can check manually.

Procedure

1. Open the appropriate port checking utility on the host system. If present, check firewall rules for the system.
2. Check the availability of ports required by Maximo Asset Management. If you find that port already assigned, ensure that you choose another value when prompted by the middleware installation program.

“Programmatically verifying prerequisites” on page 3
You can use the prerequisite verification utility to verify that installation program prerequisites are present on a system. Use this utility before starting the middleware and product installation programs.

AIX and HP-UX tar command requirements

Both the native UNIX**`tar`** command and the GNU version of the **`tar`** command are required by the middleware installation program. Because the native utility does not support long file names, ensure that GNU **`tar`** version 1.14 or higher is installed. GNU **`tar`** version 1.14 ensures that installation files can be extracted.

Verify that the system path variable contains both native UNIX **`tar`** and GNU **`tar`** paths. The GNU **`tar`** path must be defined before the native UNIX tar path. For example, the native **`tar`** utility is installed in `/usr/bin` and the GNU tar utility is installed in `/opt/freeware/bin/tar`.

If you have set a symbolic link to overwrite the native UNIX **`tar`** command with the GNU **`tar`** command an error occurs.

http://www.ibm.com/systems/p/os/aix/linux/toolbox/download.html

AIX font requirements

AIX requires specific fonts in order to produce reports.

About this task

When producing reports from AIX systems, TrueType fonts must be available on the system.

Procedure

1. Install TrueType fonts on the AIX system.
2. Ensure the fonts-path environment variable refers to the location of the fonts.

Verifying large page size support for AIX

For Maximo Asset Management to function correctly, large page size support must be enabled on AIX servers that host WebSphere Application Server.

About this task

If you are deploying Maximo Asset Management on WebSphere Application Server hosted on an AIX system, that system must be configured to support large page sizes.

Large page usage is primarily intended to provide performance improvements to high performance computing applications. Typically this feature is enabled by default on AIX systems.

Procedure

1. Log on to the AIX system that hosts WebSphere Application Server and open a console window. You must have root authority to work with the AIX operating system commands.
2. Verify large page size support by running the following command:

   ```
   ps -Z
   ```

   Output from the command includes 4K and 64K page sizes listed for processes, for example:

   ```
   # ps -Z
       PID    TTY  TIME DPGSZ SPGSZ TPGSZ CMD
    311342  pts/4  0:00    4K    4K    4K ksh
    397526  pts/4  0:00    4K    4K    4K ps
    487558  pts/4  0:00   64K   64K    4K sleep
   ```

Enabling asynchronous I/O on AIX

IBM Tivoli Directory Server requires asynchronous I/O be enabled on AIX systems.

About this task

Enabling asynchronous I/O on AIX is an installation requirement, so this step must be run before running the middleware installation program. You need to perform this step only if the system hosts the IBM Tivoli Directory Server.

Without asynchronous I/O, Oracle database instances cannot be started successfully.

To turn on asynchronous I/O follow these steps:

Procedure

1. Log in to the system as root.
2. Open a terminal and run the following command:

   ```
   smit chgaio
   ```
3. From the System Management Interface Tool (SMIT) dialog box, change STATE to be configured at system restart from **defined** to **available**.

4. Click **OK**.
5. Exit SMIT.
6. Run the following command from the command line:

   ```
   smit aio
   ```
7. In the System Management Interface Tool (SMIT) dialog box, select **Configure Defined Asynchronous I/O**, and then click **Enter**.
8. Reboot the system to enable the changes.

Checking for required libraries on Linux

The Maximo Asset Management deployment requires certain Linux system libraries.

Procedure

1. Locate the `libstdc++.so.5` library in the `/usr/lib/` directory. If this library is not installed, the middleware installation program throws an error when running the middleware installation program in graphical mode. If you cannot locate this library on your system, locate the RPM package for your system that contains this library and install the package.
2. Ensure that you have the `libstdc++33-32bit-3.3.3-11.9.x86_64.rpm` package installed before running the product installation program. SUSE Linux Enterprise Server 10 64-bit systems hosting manually configured middleware must host this package.

Configuring the JRE in Linux

In some cases, the middleware installation program fails on Red Hat Enterprise Linux 5 systems, or other systems with Security-Enhanced Linux (SELinux) enabled.

About this task

In one scenario, the middleware installation program fails with an error stating that the Java Runtime Environment (JRE) cannot be found. In another scenario, the middleware installation program fails stating that it cannot find the VM.

Complete the following steps to avoid these problems:

Procedure

1. Temporarily disable SELinux by using the **`setenforce 0`** command.
2. Run the middleware installation program.
3. Re-enable SELinux by using the **`setenforce 1`** command.
4. Manually issue the chcon -R -t textrel_shlib_t *install_home*/jvm/jre> command.

Results

The middleware installation program is now able to locate the JRE. Alternatively, you can edit the `/etc/selinux/config` file and set **`SELINUX`** to either `permissive` or `disabled` for a more permanent fix. This solution, however, affects the level of security for the entire system.

Setting the ulimit

This section details how to set the ulimit in Linux, which is used to define user system and process resource limits.

About this task

For Linux systems, you must set the ulimit for the system before using the middleware installation program.

If you set the ulimit in `.profile` for root, the ulimit setting applies to all processes.

To set the ulimit, complete the following steps:

Procedure

1. From a command line, type **`ulimit -f unlimited`**
2. From a command line, type **`ulimit -n 8192`**

Setting the swap size

Maximo Asset Management can be a resource-intensive application. Configure and tune your system for maximum performance. This section details how to set the size of the swap space used in Linux systems.

About this task

Typically, the swap size for Linux is set to twice the amount of physical RAM in the server. See the product documentation for your Linux distribution for more information.

Additional swap space can be made available to the system by:

Procedure

- increasing the size of the existing swap partition
- creating a new, additional swap partition
- creating a swap file

Setting shared memory

This section details how to set a minimum shared memory value in Linux.

About this task

For Linux systems, you must set a minimum shared memory value for the system before using the middleware installer.

To set the minimum shared memory value, complete the following steps:

Procedure

1. From a command line, type **`sysctl kernel.shmmax`** and determine if the value is less than 268435456 bytes (256 Mb).
2. If you must increase the value, from a command line, type **`sysctl -w kernel.shmmax=268435456`**.
3. Update the value in `/etc/sysctl.conf`.

Remote configuration enablement

The Maximo Asset Management installation program can automatically configure middleware. You must enable a remote access protocol for each system on which you intend to install the middleware.

Use SSH for logging on to and configuring remote Linux and UNIX systems. Use Windows SMB for logging on to and configuring remote Windows systems. Windows SMB is a Windows protocol. The IBM JRE on the administrative workstation includes SSH.

Before you start the installation program, ensure that you can log on to any remote servers with the protocols that you intend to use. Use the credentials that you plan to supply to the installation program.

For remote Windows systems, ensure that the following requirements are met before installing the software:

- The user name that you provide to the installation program must exist as a local account on the remote system. This user must be a member of the Windows Administrators group.
- The following Windows services must be started on the remote system before you begin a remote installation and configuration:
  - **`winmgmt`** (Windows Management Instrumentation)
  - **`RemoteRegistry`** (Remote Registry)
  - **`lanmanserver`** (Service)
- The SMB protocol must be enabled and configured to send NetBIOS over TCP/IP, by choosing to use port 139. Alternatively, you can configure SMB to use TCP/IP as the transport protocol, without NetBIOS, by configuring it to use port 445.
- Ensure that any ports that you use for remote protocols are not blocked by firewalls or security policies, including ports 137 and 139. Port 139 is used if SMB is configured to run on NetBIOS over TCP/IP. Port 445 is used if SMB is run directly on TCP/IP, without NetBIOS.
- To disable simple file sharing, start Windows Explorer. Click **Tools** > **Folder Options**, and clear the **Use Simple File Sharing** check box.
- The Windows administrative share (C$) and the interprocess communications (IPC$) folder must be shared.
- For Microsoft Windows Server 2008 systems that support password-protected sharing, disable password-protection. Shares must be shared for the Guest or Everyone accounts.
- For Windows systems that have User Account Control (UAC) enabled, it must be disabled before software can be remotely installed and configured.
- If Cygwin is installed on the remote Windows system the SSH daemon (sshd) must be uninstalled or disabled.

For remote Linux or UNIX systems, ensure that the following requirements are met before installing the software:

- For AIX systems, set the following SSH parameters located in the `/etc/ssh/sshd_config` file:
  - ClientAliveInterval 900
  - ClientAliveCountMax 10

  Stop the SSH daemon using the **`stopsrc -s sshd`** command and then restart it using the **`startsrc -s sshd`** command.
- For AIX systems, set the *TMOUT* and *TIMEOUT* variables in the user profile script to 0. This setting prevents the user from idling out and being logged off the remote system during the installation.

- The user name that you provide to the installation program must exist as a privileged account (for example, root) on the remote systems.
- Ensure that a current version of OpenSSH is installed and running. Do not use OpenSSH 4.7.0.5302.
- For Oracle Solaris systems, the remote access protocols require the use of internal shell scripts that must be run within the korn (ksh) shell. The methods need ksh, even if the user ID that you use to log on to the remote system is configured to use a different shell. Consequently, Oracle Solaris systems must have the ksh environment installed and properly configured.
- If you plan to remotely configure software on remote Linux or UNIX computers, ensure that SSH is installed.

Remote configuration does not support accessing network drives on the local or remote system.

Enabling SSL client authentication

The Maximo Asset Management installation program and the process solution installer fail if the client authentication feature of secure sockets layer (SSL) is enabled in the IBM HTTP Server. You can use a workaround to enable client authentication during installation.

Before you begin

The Maximo Asset Management installation and process solution installer programs use HTTP client requests for various configuration actions. The Maximo Asset Management installation program does not configure WebSphere Application Server Network Deployment nor IBM HTTP Server to use SSL. However, they do function in environments where WebSphere Application Server Network Deployment and IBM HTTP Server are manually configured to use SSL. Maximo Asset Management installation programs and standard deployment procedures do not work correctly when the client authentication feature of SSL is enabled in the IBM HTTP Server. As a result, the validation of product administration credentials or the import of data with Maximo Enterprise Adapter fails. Client authentication is enabled in the IBM HTTP Server, by using the SSLClientAuth Required directive in the `httpd.conf` configuration file.

About this task

If client authentication must be enabled for the IBM HTTP Server, use the following workaround procedure to install the product.

Procedure

1. Remove the SSLClientAuth Required directive in the `httpd.conf` configuration file of the IBM HTTP Server.
2. Stop and restart the IBM HTTP Server.
3. Run the Maximo Asset Management installation program or process solution installation programs.
4. Add the SSLClientAuth Required directive back to the `httpd.conf` configuration file of the IBM HTTP Server.
5. Stop and restart the IBM HTTP Server.

System password policy settings

Be familiar with the password policies of systems you are using as part of a Maximo Asset Management deployment.

Your organization might have password policy regulations enforced on systems on your network. Before deploying Maximo Asset Management, be sure that you are familiar with the password policies of systems used in the deployment, or you might experience errors during installation.

For example, Microsoft Windows Server 2008 systems have a stricter set of password requirements than previous versions configured by default. If you are not familiar with these stronger password requirements, you might experience an error during the installation of Maximo Asset Management. This error occurs when creating users on a Microsoft Windows Server 2008 system.

Password values that you provide during the Maximo Asset Management installation must be compliant with the password policies set for the target system. Passwords are not validated against the password policies of target systems at the time you enter them on the installation program panels. If your passwords do not conform to the password policies of systems used to deploy the product, errors occur when the installation program attempts to create these passwords during the configuration step,

Backing up the Deployment Engine database

These instructions are for backing up the Deployment Engine database. Backups are used to restore the database to the state it was before installing.

Before you begin

Back up the Deployment Engine database of the system before and after applying any updates to an existing deployment. Use backups to recover from partial installation attempts.

About this task

To back up the Deployment Engine database, complete the following steps:

Procedure

1. Set up the environment using the following command:

   Windows

   ```
   c:\install_home\ctg_DE\acsi\setenv.cmd
   ```

2. Run the command to back up the Deployment Engine registry:

   Windows

   ```
   c:\install_home\ctg_DE\acsi\bin\backupdb.cmd backup file name
   ```

   Use a meaningful name for *backup file name* to reflect the fact that it contains the state of the registry after your installation of Maximo Asset Management. For example, `DEBackupAfterInstall`.

Specifying host name values

Do not use localhost for host name values in the installation program. Specify the fully qualified host name or IP address of the system on which you are installing.

For Linux or UNIX systems, if the `hostname -f` command does not return a fully qualified host name, consult the system documentation for assistance.

Establishing a fully qualified host name on Windows systems

Use this task to establish a fully qualified host name on Windows systems.

About this task

To establish a fully qualified host name on Windows systems, complete the following steps.

Procedure

1. On the desktop, right-click **My Computer**.
2. Select Properties.
3. On the Computer Name tab, click **Change**.
4. Enter a fully qualified host name in the **Computer name** field, and then click **More**.Alternatively, you can provide the IP address for the system.
5. In the DNS Suffix and NetBIOS Computer Name window, verify that the **Primary DNS suffix** field displays a domain name, and then click **OK**.
6. In the Computer Name Changes window, click **OK**.
7. Click **Apply** and close the System Properties window.

Forcing the middleware installer to use alphanumeric hostnames

You can force the use of alphanumeric host name use within the middleware installation program by starting it from the command line and using the **`forceHostname=true`** parameter.

Example

The following example shows a use of the **`forceHostname=true`** parameter:

```
mwi-console -V forceHostname=true
```

What to do next

If you launched the middleware installation program from the command line using the **`forceHostname=true`** parameter, then you are required to provide an alphanumeric value in the **Hostname** field. An IP address results in an error message.

Launchpad

The IBM Maximo Asset Management launchpad serves as a centralized interface for launching a collection of installation programs and product information.

The launchpad application assists you in choosing which product installation programs you must install and indicates the order in which they must be installed.

Use the Maximo Asset Management launchpad to:

- start the middleware installation program.
- start the prerequisite checker utility.
- start the Maximo Asset Management installation program.
- access the Maximo Asset Management information center, including information used to plan the Maximo Asset Management installation and deployment.

Just before starting the launchpad, ensure that you meet the middleware prerequisites. Ensure that you have the correct service pack levels for your environments and always use fully qualified domain names when entering values for the installation program.

Starting the launchpad

Use the following information to start the Maximo Asset Management launchpad

Before you begin

Launchpad generated messages are captured in a hidden log frame while the launchpad is running. To show the log frame on the bottom of the launchpad panels, hold the CTRL key while simultaneously clicking the banner frame of the launchpad. Messages that are generated while the launchpad is running are not automatically saved on the hard disk drive. You can manually save the messages from a session by clicking **Save** at the bottom of the log frame and then specifying where you want to save the file.

About this task

To start the IBM Maximo Asset Management launchpad, complete the following steps:

Procedure

1. Log on to an account with system administration privileges on the computer where you want Maximo Asset Management components to be installed.
2. Start the launchpad from the root directory of the installation image:
   - Windows: Start the launchpad by using the `launchpad.exe` program.

Chapter 2. Deploy with automatic middleware configuration

Use this information to use product installation programs and tools to install and automatically configure a Maximo Asset Management deployment within your enterprise.

This information provides a high-level overview or road map of tasks you need to complete in order to deploy Maximo Asset Management with automatic middleware configuration.

In this scenario, you use the middleware installation program to install and automatically configure new instances of the following components:

- WebSphere Application Server Network Deployment
- IBM Tivoli Directory Server

You use the product installation program to perform further middleware configuration tasks automatically before finally deploying the product itself.

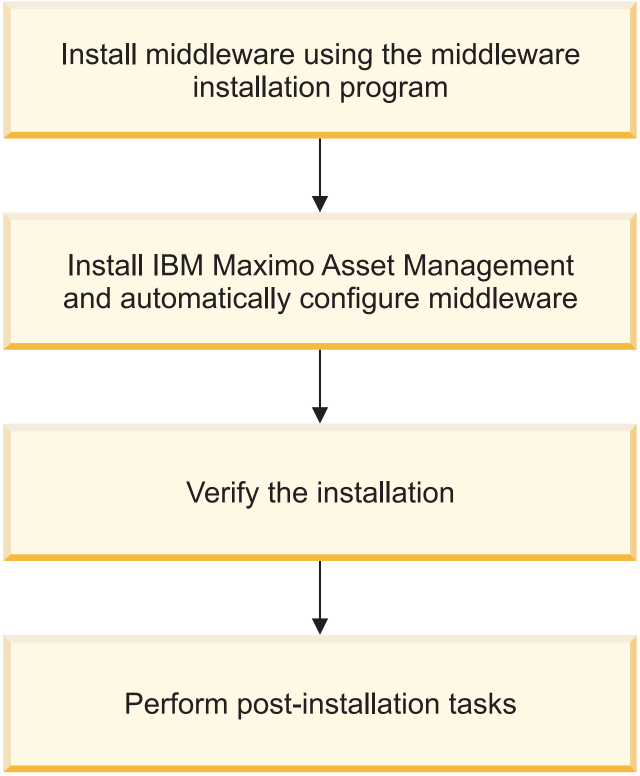
Install middleware using the middleware installation program
Install IBM Maximo Asset Management and automatically configure middleware
Verify the installation
Perform post-installation tasks

Figure 1. Deploying Maximo Asset Management using automatic middleware configuration

Middleware installation program middleware deployment plan overview

The deployment plan resides in the workspace directory and is generated from deployment choices selected in the middleware installation program.

The plan is a series of deployment steps and configuration parameters. Each step is responsible for installing and uninstalling one portion of the middleware. When deployment choices are changed, the existing deployment plan is deleted and replaced with the new deployment plan.

Installing middleware using the middleware installation program

You use the middleware installation program to install middleware components for use with IBM Maximo Asset Management. The middleware components that you choose to install, and the associated configuration parameters, are recorded in a deployment plan for the target system.

Before you begin

- Plan your installation.
- Use the planning worksheets for middleware installation to record the values that you need to specify during the installation procedure.

About this task

These instructions cover the use of the middleware installation program to install and configure middleware components on a single server. The single server deployment scenario is suitable for demonstration, test, or training purposes.

The following middleware components are installed:

- WebSphere Application Server Network Deployment
- Tivoli Directory Server

You must run the middleware installation program locally on the target system. You can start the program by using the launchpad or a setup script. When you use the launchpad, the program files are copied to a temporary directory on the target system. When you use a setup script, no files are copied to the target system. If you are installing on a 64-bit Windows system, you must use a setup script to start the program.

Procedure

1. Log in to the target system as a user with administrative authority. If you are running the middleware installation program from a Linux or UNIX terminal window, you must be logged in as the root user.
2. Start the middleware installation program by using the launchpad or a setup script.
   - Use the launchpad to start the middleware installation program.
     a. Start the launchpad.

        Windows (32-bit only)
        From the root directory of the installation image, run the following command: `launchpad.exe`.

        Linux and UNIX
        From the root directory of the installation image or product media, run the following command: `launchpad.sh`.

     b. Run the middleware installation requirements checking utility.

     c. Click **Middleware**.
   - Run the following command to launch a setup script which starts the middleware installation program:

Windows

```
launchpad\Install\MWI\setupwin.bat /l
```

Linux and UNIX

```
launchpad/Install/MWI/setupUNIX.sh -l
```

3. Specify the workspace location for this installation of middleware.
4. On the Deployment Choices panel, select the components that you want to install on this system.
5. Review the summary of the generated deployment plan and click **Next** to proceed with configuration of the specified components. When you click **Next**, the middleware installation program verifies the prerequisites for installing the specified components.
6. To specify a host name for the target system other than the default host name, select **Override the local machine hostname** and enter a host name in the **Hostname** field. You cannot clear this option after it has been selected, however, you can change the value in the **Hostname** field.
7. Optional: To specify a default password that can be used throughout the middleware installation program, select **Use this password as the value for all subsequent passwords** and enter the required password.
8. Specify the following details for IBM Tivoli Directory Server:
   a. Specify the installation directory.
   b. Specify a distinguished name and password for the Tivoli Directory Server administrator.
9. Specify the configuration parameters that are required for Tivoli Directory Server, including the organizational unit, organization suffix, and country suffix that are required when the directory server is used with Maximo Asset Management.
10. Specify the following details for the Tivoli Directory Server database instance:
    a. Specify the name of the DB2® database that you are using to hold Tivoli Directory Server data.
    b. Specify the name and password of the Tivoli Directory Server database instance.
11. Specify the configuration parameters that are required when Tivoli Directory Server is being used as the LDAP resource for WebSphere Application Server Network Deployment security.
12. Specify the bind distinguished name and password that are required for binding to the LDAP instance. When you click **Next**, the middleware installation program validates the host and directory information that you specified for the directory server. The specified information must be verified before the installation can proceed.
13. Specify the install location and administrative account details for WebSphere Application Server Network Deployment.
14. Specify the profile names for the WebSphere Application Server Network Deployment deployment manager and application servers.
15. Specify the following details for WebSphere Application Server Network Deployment:
    a. Specify the WebSphere Application Server Network Deployment cell name.
    b. Specify the names of the WebSphere Application Server Network Deployment deployment manager and application server nodes.
    c. Specify the install location WebSphere Application Server Network Deployment update installer.

16. Specify the install location, the port used by IBM HTTP Server, and the port that must be used to administer IBM HTTP Server. If you install IBM HTTP Server into a directory path that includes spaces, for example, the default install location for Windows systems, you cannot start and stop it from the administrative console. If the directory path includes spaces, you must start and stop the IBM HTTP Server from the command line.
17. Accept the default profile name for the WebSphere Application Server Network Deployment plug-in for IBM HTTP Server by clicking **Next**. This value cannot be changed.
18. Specify whether you need to copy the Maximo Asset Management middleware installation images from the product media to your file system:
    - If you need to copy the middleware installation images from the product media, specify the source and destination directories.
    - If the middleware installation images are already saved to the file system, specify the directory where they are located.
19. Optional: Before you deploy, verify the integrity of the middleware installation images by selecting the option for checksum validation. If the checksum operation fails, click **Back** and recopy the images. If you do not select this option and the middleware installation images are corrupted or otherwise inaccessible from the directory specified, an error occurs. If you encounter this error, you must replace the corrupted middleware installation images and then restart the middleware installation program.
20. Specify a directory to use for middleware installation program temporary files and extracted middleware installation images.
21. Select **Deploy the plan** to confirm that you are ready to install and configure the selected middleware components.
22. Click **Deploy** to initiate the installation process.
23. When the deployment is complete, click **Finish** to close the installation wizard.

Middleware installation program logs

Middleware installation program log files are in the workspace directory that was defined in the middleware installation program.

There are several types of log files.

User interface logs

The logs generated by the middleware installation program user interface are in the workspace directory.

The middleware installation program logs all information in `<workspace_loc>/mwi.log`: Default workspace locations for all platforms are as follows:

Windows
`C:\ibm\tivoli\mwi\workspace`

Linux `/root/ibm/tivoli/mwi/workspace`

AIX `/ibm/tivoli/mwi/workspace`

The `mwi.log` file is the high-level log file that was generated by the most recent invocation of the middleware installation program. If an error occurs, examine this log file first. An entry in this log file might direct you to a lower-level log file.

Log files named mwi.log*X*, where *X* is a number, are copies of the mwi.log file from earlier invocations of the middleware installation program. So, for example, mwi.log0 is produced after the first invocation of the middleware installation program. mwi.log1 is produced after the second invocation of the middleware installation program.

Logs for steps run by the user interface

In addition to collecting input from the user, the user interface of the middleware installation program also performs several system checks. Examples of system checks run by the user interface runs include:

- dependency checking to ensure that the operating system meets the deployment requirements
- inventorying the software on the system to locate existing instances of middleware products deployed by the middleware installation program
- checking the available disk space to ensure that there is enough for the deployment

Each of these checks is produced in the form of a step so that it can also be run as part of the deployment plan. When the user interface runs a step, it copies the step into a subdirectory of the workspace directory. The log files generated by a step are in the same subdirectory. These files follow the same pattern as a step that is run as part of the deployment plan.

Logs for the deployment plan

The deployment plan is in the directory *<Workspace Directory>*/*host name*/deploymentPlan, where *host name* is the host name of the current system. Each time the deployment plan is used to install or uninstall middleware products, a process ID is assigned and log files are generated.

The log files for the deployment plan are in the subdirectory logs/*processID*. The primary log file for the deployment plan is DeploymentPlan.log, a high-level log file that lists the steps started as part of the deployment plan.

Logs for the workstation plan

The machine plan is located in the directory *<Workspace Directory>*/*host name*/deploymentPlan/MachinePlan_*host name*. The log files for the machine plan are in the logs subdirectory. The primary log files for the machine plan are named MachinePlan_*host name*_*processID*. These log files contain the output generated by Apache ANT when running the machine plan ANT script.

Logs for steps in the deployment plan

Each step in the deployment plan is in a directory named *<Workspace Directory>*/*host name*/deploymentPlan/MachinePlan_*host name*/*stepNum*_*stepID*, where *stepNum* is the sequence number of this step in installation processing order of the deployment plan and *stepID* identifies the step. The log files for the step are in the logs subdirectory.

Some steps might provide a message log file named *stepID*_*processID*.message, which contains a few entries that summarize the result of starting the step. All steps provide a trace log file named *stepID*_*processID*.log, which contains many entries, typically including information about the input parameters and the substeps started.

Logs for substeps

Each step contains one or more substeps. The substeps perform the actual installation, uninstall, and checking work for the middleware installation program.

Each substep is in the directory *<Workspace Directory>*/*host name*/deploymentPlan/MachinePlan_*host name*/*stepNum_stepID*/*operation*/*substepNum_substepID*, where *operation* is the ANT target in the step ANT script that starts this substep. *substepNum* is the sequence number of this substep in the processing order of the step, and *substepID* identifies the substep. Typical values for operation are install, uninstall, and check.

The log files for the substep are typically in a subdirectory named *processID*/logs.

Log files generated by the native middleware installation programs are also kept here.

Middleware installation program log reference

The following logs are produced during the use of the middleware installation program.

IBM Tivoli Directory Server DB2 for Maximo Asset Management Step

The following IBM Tivoli Directory Server DB2 for Maximo Asset Management logs can be found in <*workspace*>/<*machine_name*>/deploymentPlan/MachinePlan_<*machine_name*>/000*XX*_ITDS_DB2_CCMDB/check/01_CHECKS/<*Time_Stamp*>/logs:

- etcgroupfile.log
- etcpasswdfile.log

IBM Tivoli Directory Server Installation Step

IBM Tivoli Directory Server installation logs can be found in the following locations:

GSKIT

The following IBM Tivoli Directory Server installation log files can be found in the <*workspace*>/<*machine_name*>/deploymentPlan/MachinePlan_<*machine*_name>/000*XX*_ITDS_6.3/install/01_GSKIT/<*Time_Stamp*>/logs directory.

- de_processreq.log
- de_trace.log

For Windows and Linux, including Linux on IBM System z®, the following additional files are produced:

- GSKit_Install_GSKit_<*Time_Stamp*>.log
- GSKit_Install_GSKit_<*Time_Stamp*>.err

For 32-bit Windows systems, the following additional file is produced:

- gskInstall.log

For 32-bit Windows systems, the following additional files are produced:

- ISScript_Install.log
- gskInstall.log

For AIX systems, the following additional files are produced:

- GSKit_Install_JS_RTE_20080721_084044GMT-06.00.log
- GSKit_Install_SA_RTE_20080721_084044GMT-06.00.log
- •GSKit_Install_TA_RTE_20080721_084044GMT-06.00.log
- rteList.log

The `de_processreq.log` contains status information. This log file provides details on which action has failed. The failed action log can be examined for more information.

IBM Tivoli Directory Server base

The following IBM Tivoli Directory Server base log files can be found in the `<workspace>/<machine_name>/deploymentPlan/MachinePlan_<machine_name>/000XX_ITDS_6.3/install/02_BASE/<Time_Stamp>/logs` directory:

- `de_processreq.log`
- `de_trace.log`

For Windows, the following additional files are available:

- `ldapinst.log`
- `registryList.log`

For Linux, including Linux on IBM System z, the following additional files are produced:

- `ITDS6.3_CheckRPMEntry_<Time_Stamp>.err`
- `ITDS6.3_CheckRPMEntry_<Time_Stamp>.log`
- `rpmList.log`

For AIX systems, the following additional files are produced:

- `ITDS6.3_CheckRTEEntry_<Time_Stamp>.log`
- `ITDS6.3_CheckRTEEntry_<Time_Stamp>.err`
- `rteList.log`

The `de_processreq.log` contains status information. This log file provides details on which action has failed. The failed action log can be examined for more information.

IBM Tivoli Directory Server fix pack

The following IBM Tivoli Directory Server fix pack log files can be found in the <*workspace*>/<*machine_name*>/deploymentPlan/MachinePlan_<*machine_name*>/000XX_ITDS_6.3/install/02A_FP/<*Time_Stamp*>/logs directory:

- `de_processreq.log`
- `de_trace.log`

For Windows, the following additional file are available:

- `ldapinst.log`

For Linux, the following additional files are produced:

- `ITDS6.3_CheckRPMEntry_<Time_Stamp>.err`
- `ITDS_InstallFixpack_<Time_Stamp>.log`
- `rpmList.log`

For AIX systems, the following additional files are produced:

- `ITDS_InstallFixpack_<Time_Stamp>.err`
- `ITDS_InstallFixpack_<Time_Stamp>.log`
- `ITDS6.3_CheckRTEEntry_<Time_Stamp>.log`
- `ITDS6.3_CheckRTEEntry_<Time_Stamp>.err`
- `rteList.log`

The de_processreq.log contains status information. This log file provides details on which action has failed. The failed action log can be examined for more information.

IBM Tivoli Directory Server language pack

The following IBM Tivoli Directory Server language pack log files can be found in the *<workspace>*/*<machine_name>*/deploymentPlan/MachinePlan_*<machine_name>*/000XX_ITDS_6.3/install/03_LP/*<Time_Stamp>*/logs directory:

- de_processreq.log
- de_trace.log

For Windows, the following additional files are available:

- ldapLP_inst.log
- registryList.log

For Linux, including Linux on IBM System z, the following additional file is produced:

- checkIfRPMEntryExists_*<Time_Stamp>*.log

For AIX systems, the following additional files are produced:

- checkIfRTEEntryExists_*<Time_Stamp>*.log
- checkIfRTEEntryExists_*<Time_Stamp>*.err

IBM Tivoli Directory Server Configuration Step

The following IBM Tivoli Directory Server configuration logs can be found in *<workspace>*/*<machine_name>*/deploymentPlan/MachinePlan_*<machine_name>*/000*XX*_ITDS_Configuration/install/01_CONFIG/logs:

- createUsers.log
- netUserCheck.log

For Windows, the following additional files are produced:

- PasswdNeverExpires.log
- configureDB.log (produced in the 02_CONFIG folder)
- configureDNPassword.log (produced in the 02_CONFIG folder)
- configureSuffix.log (produced in the 02_CONFIG folder)
- startInstanceTool.log (produced in the 02_CONFIG folder)
- startServer.log (produced in the 02_CONFIG folder)
- audit.log (produced in the C:\idsslapd-idsccmdb\logs folder)
- bulkload.log (produced in the C:\idsslapd-idsccmdb\logs folder)
- db2clicmds.log (produced in the C:\idsslapd-idsccmdb\logs folder)
- lostandfound.log (produced in the C:\idsslapd-idsccmdb\logs folder)
- traceibmslapd.log (produced in the C:\idsslapd-idsccmdb\logs folder)
- adminaudit.log (produced in the C:\idsslapd-idsccmdb\logs folder)
- ibmdiradm.log (produced in the C:\idsslapd-idsccmdb\logs folder)
- db2cli.log (produced in the C:\idsslapd-idsccmdb\logs folder)
- perftune_stat.log (produced in the C:\idsslapd-idsccmdb\logs folder)
- idstools.log (produced in the C:\idsslapd-idsccmdb\logs folder)

For UNIX, including Linux,Linux on IBM System z, and AIX, the following additional files are produced:

- permissions.log
- ITDS_LDAP_Config.encrypted.ldif (produced in the 03_CONFIG folder)
- addLDIFData.log (produced in the 03_CONFIG/logs folder)
- idsadm.log (produced in the /var/idsldap/V6.3 folder)
- idsadmdb2.log (produced in the /var/idsldap/V6.3 folder)
- idsadmdb2cmds.log (produced in the /var/idsldap/V6.3 folder)

WebSphere Application Server Network Deployment Installation Step

WebSphere Application Server Network Deployment installation logs can be found in the following locations:

WebSphere Application Server Network Deployment

The following WebSphere Application Server Network Deployment installation log files can be found in the <*workspace*>/<*machine_name*>/deploymentPlan/MachinePlan_<*machine*_name>/000*XX*_WAS_ND_7.0/install/01_BASE/<*Time_Stamp*>/logs directory.

- de_processreq.log
- de_processreq.log_utf8
- de_trace.log
- ProductInstall.log
- WAS_ND_InstallProduct_<*Time_Stamp*>.err
- WAS_ND_InstallProduct_<*Time_Stamp*>.log

UpdateInstaller

The following UpdateInstaller installation log files can be found in the <*workspace*>/<*machine_name*>/deploymentPlan/MachinePlan_<*machine*_name>/000*XX*_WAS_ND_7.0/install/01_UPDT_INST/<*Time_Stamp*>/logs directory.

- de_processreq.log
- de_processreq.log_utf8
- de_trace.log
- ProductInstall.log
- Update_Installer_InstallProduct_<*Time_Stamp*>.err
- Update_Installer_InstallProduct_<*Time_Stamp*>.log
- UpdateInstaller_MoveUpdateInstallerInstallLogsToLogsLoc.err
- UpdateInstaller_MoveUpdateInstallerInstallLogsToLogsLoc.log

The de_processreq.log contains status information. This log file provides details on which action has failed. The failed action log can be examined for more information. The ProductInstall.log file is the native log for the fix pack. This log contains WebSphere Network Deployment and UpdateInstaller installation information.

WebSphere Application Server Network Deployment Configuration Step

WebSphere Application Server Network Deployment configuration logs can be found in the <*workspace*>/<*machine_name*>/deploymentPlan/MachinePlan_<*machine*_name>/000*XX*_WAS_ND_Configuration/install/01_CONFIG/<*Time_Stamp*>/logs directory:

- createAppServer.log

- MXServer_serverStatus.log
- nodeagent_serverStatus.log
- setupcmd.log
- startManager.log
- startServer.log
- UnixAugmentProfileDMgrForISC.log
- UnixCreateProfileAppSvr.log
- UnixCreateProfileDMgr.log
- verifyProfile.log
- startManager.log (produced in the 02_CONFIG folder)
- stopManager.log (produced in the 02_CONFIG folder)
- stopNode.log (produced in the 02_CONFIG folder)
- syncNode.log (produced in the 02_CONFIG folder)
- VMMConfigData.log (produced in the 02_CONFIG folder)
- SystemErr.log (produced in the <*WAS_HOME*>/profiles/ctgDmgr01/logs/dmgr folder)
- SystemOut.log (produced in the <*WAS_HOME*>/profiles/ctgDmgr01/logs/dmgr folder)
- addNode.log (produced in the <*WAS_HOME*>/profiles/ctgAppSrv01/logs folder)
- runAddNode.log (produced in the <*WAS_HOME*>/profiles/ctgAppSrv01/logs folder)
- syncNode.log (produced in the <*WAS_HOME*>/profiles/ctgAppSrv01/logs folder)
- wsadmin.traceout (produced in the <*WAS_HOME*>/profiles/ctgAppSrv01/logsfolder)
- SystemErr.log (produced in the <*WAS_HOME*>/profiles/ctgAppSrv01/logs/nodeagent folder)
- SystemOut.log (produced in the <*WAS_HOME*>/profiles/ctgAppSrv01/logs/nodeagent folder)
- startServer.log (produced in the <*WAS_HOME*>/profiles/ctgAppSrv01/logs/MXServer folder)
- stopServer.log (produced in the <*WAS_HOME*>/profiles/ctgAppSrv01/logs/MXServer folder)
- SystemErr.log (produced in the <*WAS_HOME*>/profiles/ctgAppSrv01/logs/MXServer folder)
- SystemOut.log (produced in the <*WAS_HOME*>/profiles/ctgAppSrv01/logs/MXServer folder)

IBM HTTP Server Installation Step

IBM HTTP Server installation logs can be found in the following locations:

IBM HTTP Server Base

The following IBM HTTP Server base installation log files can be found in the <*workspace*>/<*machine_name*>/deploymentPlan/MachinePlan_<*machine*_name>/000*XX*_IHS_7.0/install/01_BASE/<*Time_Stamp*>/logs directory.

- de_processreq.log
- de_processreq.log_utf8

- `de_trace.log`
- `IHS_InstallProduct_<`*`Time_Stamp`*`>.err`
- `IHS_InstallProduct_<`*`Time_Stamp`*`>.log`
- `ProductInstall.log`

The `de_processreq.log` contains status information. This log file provides details on which action has failed. The failed action log can be examined for more information. `ProductInstall.log` is the native product log. This log contains IBM HTTP Server installation information.

IBM HTTP Server fix pack

The following IBM HTTP Server fix pack log files can be found in the <*workspace*>/<*machine_name*>/deploymentPlan/ MachinePlan_<*machine_name*>/000XX_IHS_7.0/install/01A_FP/ <*Time_Stamp*>/logs directory:

- `de_processreq.log`
- `de_processreq.log_utf8`
- `de_trace.log`
- `IHS_Fixpack_GetIHSUpdateVersion_<`*`Time_Stamp`*`>.err`
- `IHS_Fixpack_GetIHSUpdateVersion_<`*`Time_Stamp`*`>.log`
- `IHS_Fixpack_InstallIHSFixpack_<`*`Time_Stamp`*`>.err`
- `IHS_Fixpack_InstallIHSFixpack_<`*`Time_Stamp`*`>.log`
- `IHS_Fixpack_MoveIHSFixInstallLogsToLogsLoc_<`*`Time_Stamp`*`>.err`
- `IHS_Fixpack_MoveIHSFixInstallLogsToLogsLoc_<`*`Time_Stamp`*`>.log`

For Windows, the following additional files are available:

- `IHS_Fixpack_StartIHSAdminService_<`*`Time_Stamp`*`>.err`
- `IHS_Fixpack_StartIHSAdminService_<`*`Time_Stamp`*`>.log`
- `IHS_Fixpack_StartService_<`*`Time_Stamp`*`>.err`
- `IHS_Fixpack_StartService_<`*`Time_Stamp`*`>.log`
- `IHS_Fixpack_StopIHSAdminService_<`*`Time_Stamp`*`>.err`
- `IHS_Fixpack_StopIHSAdminService_<`*`Time_Stamp`*`>.log`
- • `IHS_Fixpack_StopService_<`*`Time_Stamp`*`>.err`
- • `IHS_Fixpack_StopService_<`*`Time_Stamp`*`>.log`

For UNIX, including Linux,Linux on IBM System z, and AIX, the following additional files are produced:

- `IHS_Fixpack_StartServiceLinux_<`*`Time_Stamp`*`>.err`
- `IHS_Fixpack_StartServiceLinux_<`*`Time_Stamp`*`>.log`
- `IHS_Fixpack_StopServiceLinux_<`*`Time_Stamp`*`>.err`
- `IHS_Fixpack_StopServiceLinux_<`*`Time_Stamp`*`>.log`
- `ProductInstall.log`

The `de_processreq.log` contains status information. This log file provides details on which action has failed. The failed action log can be examined for more information. `ProductInstall.log` is the native product log. This log contains IBM HTTP Server fix pack installation information.

WebSphere plug-ins

The following WebSphere plug-in logs can be found in the <*workspace*>/<*machine_name*>/deploymentPlan/ MachinePlan_<*machine_name*>/000XX_IHS_7.0/install/02_WAS_PLUGIN/ <*Time_Stamp*>/logs directory:

- de_processreq.log
- de_processreq.log_utf8
- de_trace.log
- ProductInstall.log
- WAS_plugins_for_WAS_InstallProduct_<*Time_Stamp*>.err
- WAS_plugins_for_WAS_InstallProduct_<*Time_Stamp*>.log

The de_processreq.log contains status information. This log file provides details on which action has failed. The failed action log can be examined for more information. ProductInstall.log is the native product log. This log contains IBM HTTP Server fix pack installation information.

WebSphere plug-in fix pack

The following WebSphere plug-in logs can be found in the <*workspace*>/<*machine_name*>/deploymentPlan/ MachinePlan_<*machine_name*>/000*XX*_IHS_7.0/install/02A_FP/ <*Time_Stamp*>/logs directory:

- de_processreq.log
- de_processreq.log_utf8
- de_trace.log
- ProductInstall.log
- WAS_Plugins_for_WAS_Fixpack_GetWASPluginUpdateVersion_ <*Time_Stamp*>.err
- WAS_Plugins_for_WAS_Fixpack_GetWASPluginUpdateVersion_ <*Time_Stamp*>.log
- WAS_Plugins_for_WAS_Fixpack_InstallWASPluginsFixpack_ <*Time_Stamp*>.err
- WAS_Plugins_for_WAS_Fixpack_InstallWASPluginsFixpack_ <*Time_Stamp*>.log
- WAS_Plugins_for_WAS_Fixpack_MoveIHSFixInstallLogsToLogsLoc_ <*Time_Stamp*>.err
- WAS_Plugins_for_WAS_Fixpack_MoveIHSFixInstallLogsToLogsLoc_ <*Time_Stamp*>.log

The de_processreq.log contains status information. This log file provides details on which action has failed. The failed action log can be examined for more information. ProductInstall.log is the native product log. This log contains IBM HTTP Server fix pack installation information.

For Windows, the following additional files are available:

- WASPlugin _Fixpack_StartIHSAdminService_<*Time_Stamp*>.err
- WASPlugin _Fixpack_StartIHSAdminService_<*Time_Stamp*>.log
- WASPlugin _Fixpack_StartService_<*Time_Stamp*>.err
- WASPlugin _Fixpack_StartService_<*Time_Stamp*>.log
- WASPlugin _Fixpack_StopIHSAdminService_<*Time_Stamp*>.err
- WASPlugin _Fixpack_StopIHSAdminService_<*Time_Stamp*>.log
- WASPlugin _Fixpack_StopService_<*Time_Stamp*>.err
- WASPlugin _Fixpack_StopService_<*Time_Stamp*>.log

For UNIX, including Linux,Linux on IBM System z, and AIX, the following additional files are produced:

- WASPlugin_Fixpack_StartServiceLinux_<*Time_Stamp*>.err

- WASPlugin_Fixpack_StartServiceLinux_<*Time_Stamp*>.log
- WASPlugin_Fixpack_StopServiceLinux_<*Time_Stamp*>.err
- WASPlugin_Fixpack_StopServiceLinux_<*Time_Stamp*>.log

The de_processreq.log contains status information. This log file provides details on which action has failed. The failed action log can be examined for more information. ProductInstall.log is the native product log. This log contains IBM HTTP Server fix pack installation information.

IBM HTTP Server WebSphere plug-in configuration

The following IBM HTTP Server WebSphere plug-in configuration logs can be found in the <*workspace*>/<*machine_name*>/deploymentPlan/MachinePlan_<*machine_name*>/000XX_IHS_7.0/install/03_CONFIG/<*Time_Stamp*>/logs directory:

- configure.webserver.command.out
- ConfigureIHSPlugin.out
- start.http.server.out
- SystemErr.log (produced in the <*WAS_HOME*>/profiles/ctgDmgr01/logs/dmgr folder)
- SystemOut.log (produced in the <*WAS_HOME*>/profiles/ctgDmgr01/logs/dmgr folder)

Authentication service

Authentication service logs can be found in the <*workspace*>/<*machine_name*>/deploymentPlan/MachinePlan_<*machine*_name>/000*XX*_ESS_*XX*/install/01_CONFIG/<*Time_Stamp*>/logs directory:

- configureESS.log
- exportWASLTPAKeys.log
- importLTPAKeys.log
- installESS.log
- installWIM.log
- key.file
- modifyLTPASettings.log
- save.log
- startManager.01.log
- startManager.02.log
- startNode.01.log
- startNode.02.log
- startServer.01.log
- startServer.02.log
- stopManager.01.log
- stopManager.02.log
- stopNode.01.log
- stopNode.02.log
- stopServer.01.log
- stopServer.02.log
- sync.log
- SystemErr.log (produced in the <*WAS_HOME*>/profiles/ctgDmgr01/logs/dmgr/ folder)

- SystemOut.log (produced in the <*WAS_HOME*>/profiles/ctgDmgr01/logs/dmgr/ folder)
- addNode.log (produced in the <*WAS_HOME*>/profiles/ctgAppSrv01/logs/ folder)
- runAddNode.log (produced in the <*WAS_HOME*>/profiles/ctgAppSrv01/logs/ folder)
- syncNode.log (produced in the <*WAS_HOME*>/profiles/ctgAppSrv01/logs/ folder)
- wsadmin.traceout (produced in the <*WAS_HOME*>/profiles/ctgAppSrv01/logs/ folder)
- SystemErr.log (produced in the <*WAS_HOME*>/profiles/ctgAppSrv01/logs/nodeagent/ folder)
- SystemOut.log (produced in the <*WAS_HOME*>/profiles/ctgAppSrv01/logs/nodeagent/ folder)
- SystemErr.log (produced in the <*WAS_HOME*>/profiles/ctgAppSrv01/logs/MXServer/ folder)
- SystemOut.log (produced in the <*WAS_HOME*>/profiles/ctgAppSrv01/logs/MXServer/ folder)

Configuring IBM Tivoli Directory Server user and group strings

You can configure user and group strings in IBM Tivoli Directory Server to adapt it to your deployment needs.

About this task

You can manually create user and group strings for Tivoli Directory Server during installation.

If you configure directory server user and group strings for a system that hosts only the IBM Tivoli Directory Server , you must manually create properties in the input.properties file of the ITDS_CONFIGURATION step of the deployment plan.

Procedure

1. Edit the input.properties file that is in the directory server folder at: *Workspace*\machine name\deploymentPlan\MachinePlan_*machine shortname*\00006_ITDS_Configuration. For example, in Windows, the default location of the input.properties file is C:\ibm\tivoli\mwi\workspace\mymachine.ibm.com\deploymentPlan\MachinePlan_mymachine\00006_ITDS_Configuration.
2. Add the following properties:
   ```
   was_nd.secure.GroupSuffix=ou\=groups,ou\=SWG,o\=IBM,c\=US
   was_nd.secure.UserSuffix=ou\=users,ou\=SWG,o\=IBM,c\=US
   ```
3. If Tivoli Directory Server configuration parameters are customized, change the applicable values to your custom values on the configuration parameters panel. For example, if your custom values are ou=SWG1 and the Organization country suffix is o=IBM1,c=US1, you must manually replace all occurrences of those values in the input.properties file:
   ```
   was_nd.secure.GroupSuffix=ou\=groups,ou\=SWG1,o\=IBM1,c\=US1
   was_nd.secure.UserSuffix=ou\=users,ou\=SWG1,o\=IBM1,c\=US1
   ```

Uninstalling middleware

To uninstall IBM Maximo Asset Management middleware, you must run the middleware installation program and select the options to remove the previous deployment.

Before you begin

If you chose to deploy Maximo Asset Management middleware with a directory server, ensure that it is active. You must remove the J2EE server before you can remove the directory server.

About this task

The middleware installation program creates a registry when installing Maximo Asset Management middleware. Using the native middleware uninstall programs causes this registry to be out of sync with what is deployed. As a result, errors occur when you attempt to reinstall middleware with the middleware installation program.

Procedure

1. Stop and start servers as required:
   a. Stop the IBM Tivoli Directory Server (IBM Tivoli Directory Server v6.3 - idsccmdb).
   b. Stop the IBM Tivoli Directory Server daemon (IBM Tivoli Directory Admin Server v6.3 - idsccmdb).
   c. Start DB2.
   d. Start the idsccmdb DB2 instance (DB2 - DB2COPY1 - IDSCCMDB).
   e. Start the IBM Tivoli Directory Server daemon (IBM Tivoli Directory Admin Server v6.3 - idsccmdb)
2. Log in as Administrator on Windows and root on Linux and AIX.
3. Start the launchpad by running the following command from the root directory of the downloaded installation image:

Option	Description
Windows	`launchpad.exe`
Linux	`launchpad.sh`
AIX	`launchpad.sh`

4. In the launchpad navigation pane, click **Install Product**.
5. In the Install the middleware section, click **Middleware** and step through the launchpad panels.
6. When you are prompted to browse to a workspace, specify the workspace directory that contains the currently deployed plan, and click **Next**. The default location for the workspace is the last workspace location specified. If you did not specify a path previously, the default location for the workspace `isc:\ibm\tivoli\mwi\workspace`
7. In the Select Operation panel, select **Undeploy the plan**, and click **Next**.
8. From the undeployment preview panel, click **Next** to undeploy the plan.
9. Exit the middleware installation program.

Installation program overview

The Maximo Asset Management installation program provides an interface for installing and deploying Maximo Asset Management, which includes the process automation engine and process managers.

The Maximo Asset Management installation program records choices you make about your Maximo Asset Management deployment. It records configuration parameters associated with those choices, and then installs and deploys Maximo Asset Management based upon the information you entered.

There are two installation paths available to you when you are installing Maximo Asset Management.

Simple

A simple deployment consists of installing Maximo Asset Management middleware on one system. You do not have the option of using existing middleware within your organization with Maximo Asset Management. All middleware used with Maximo Asset Management must be installed on the system with the middleware installation program with default values. Maximo Asset Management is installed with default values provided by the middleware installation program and Maximo Asset Management installation program.

If you intend to override default values used by the simple deployment path, you must use the custom deployment path instead.

Custom

A custom deployment typically involves deploying Maximo Asset Management across several systems. Some of these systems might already host middleware products that you want to use with your Maximo Asset Management deployment. You can modify default installation values when you deploy with the custom installation path.

This deployment option does not require you to spread the Maximo Asset Management deployment across several systems. You can enter the name of the local host as the destination for all Maximo Asset Management components.

The Maximo Asset Management installation program can automate the configuration of some middleware for use with Maximo Asset Management.

If you choose not to have the Maximo Asset Management installation program automatically configure middleware, you must configure that piece of middleware manually **before** the installation of Maximo Asset Management.

Important: When you are entering LDAP values for Maximo Asset Management installation panel fields, be aware of the product-specific syntax rules for using special characters in an LDAP string. In most cases, special characters must be preceded by an escape character in order to make it readable by the directory server. Failing to escape special characters contained in an LDAP string used with Maximo Asset Management results in Maximo Asset Management errors.

Many directory server products consider a blank space as a special character that is part of the LDAP string. If you enter an LDAP string with an unescaped blank character at the end of a field value, you encounter Maximo Asset Management errors.

For more information about special character usage in LDAP strings, see the product documentation for your directory server.

Information that you enter for the Maximo Asset Management installation program is stored in the `maximo.properties` and `install.properties` files and the Maximo database. These values are populated into the panel fields of the Maximo Asset Management installation program on subsequent uses of the program. If you cancel the installation program, it recalls most values that you entered the next time you start it. Values excluded from being saved in this manner are the Maximo Asset Management installation directory and the shortcut option chosen during the installation. You can restore the default values in the Maximo Asset Management installation program by deleting `<`*`Maximo_Home`*`>/applications/maximo/properties/maximo.properties` and `<`*`Maximo_Home`*`>/etc/install.properties`. If you cannot locate the `maximo.properties` file in the `<Maximo_Home>` directory, look for it in the system temp file directory.

Installing the product and automatically configuring middleware

To install Maximo Asset Management, you run the installation program from the launchpad. The installation procedure automatically configures middleware on multiple servers, using default values.

Before you begin

Ensure that you meet prerequisite conditions.

- The database server, the directory server, and application server services must be started and active.
- On the administrative workstation, temporarily shut down any noncritical processes that can have a negative effect on the installation, such as antivirus software.
- Ensure that the Windows DEP setting does not prevent the launchpad from running: Select **Start** > **Settings** > **Control Panel** > **System** > **Advanced** > **Performance** > **Settings** > **Data Execution Prevention**. Select **Turn on DEP for essential Windows programs and services only** and click **Apply**. You might be asked to reboot the server.
- For Linux and UNIX systems with middleware installed, the command **`hostname -f`** must return a fully qualified host name. If necessary, consult the documentation for your operating system. Alternatively, you can provide the IP address for the system.
- Enable a remote execution and access service on every system that has middleware installed. Each remote system must support a remote access protocol. It must also accept remote logins from a user name and password that were configured on the target server. Remote access protocols include SSH and Windows SMB. If the remote system is a Windows server, you must configure remote execution and access to use SMB.

About this task

The instructions are for a multiple server installation that uses default values.

Procedure

1. Log in on the administrative system.
2. Start the product installation program from the launchpad.

a. Start the launchpad. Browse to the root directory of the downloaded installation image, and run the following command:

   Windows

   ```
   launchpad.exe
   ```

b. In the launchpad navigation pane, click **Install Product**.

c. Click **Install Maximo Asset Management 7.5**.

If the launchpad does not start the installation, you can start the product installation program directly. On the downloaded installation image, browse to `\Install\mam\`, and run one of the following commands:

Windows

- `install.bat`
- `install_win64.bat`

3. Select a language for the installation and click **OK**.
4. On the Choose Installation Folder panel, specify the path to the location where you want to install Maximo Asset Management.

   You can specify a description for the installation. A description is useful for differentiating between multiple installations that are hosted on the same administrative workstation.
5. Review the information that is on the Verify Installation Location panel. The panel shows any previous installation information that was found based on the installation directory that you specified on the previous panel. After you advance past this panel, you cannot go back and change the installation directory for this installation.

   If a more recent version of the installation program is found in the specified target directory, you are notified. The notification means that you are using an older version of the installation program. The version found on the administrative workstation is newer and can contain important features and enhancements. To use the newer version of the installation program, select the option on the notification panel and click **Next**. This action exits the current installation process and restarts the installation process with the newer installation program. If you do not select the option, you continue the installation with the older version of the installation program.
6. On the Package Summary panel, review the package deployment information. This panel lists version information for both new and existing packages on the system. Target package version information indicates the package version being currently deployed.
7. On the Choose Deployment panel, specify **Simple** or **Custom** as the deployment type.
8. On the Import Middleware Configuration Information panel, you select **Import middleware configuration information** to have the product installation program reuse the middleware installation program values. These values are used as default values for the same fields in the product installation program.

   The **Workspace location** field refers to the location of the topology file that contains the values that were specified for the middleware installation program. The file is located in the workspace that was defined during the middleware installation task. For example, `C:\ibm\tivoli\mwi\workspace` for Windows or `/root/ibm/tivoli/mwi/workspace` for UNIX.

   If you selected the simple deployment, the middleware default information is not used.

9. On the Database Type panel, specify the software to use for the Maximo database.
10. On the Database panel, specify configuration information for your database software.

    For things such as the database user ID, the database name, the database instance for Maximo Asset Management, and the schema name, if the values do not exist when you specify them, they are created.

    Database users and database instance names cannot contain spaces.

    After you specify configuration information for your database software, the installation program validates the information with the database server.
11. On the Automate Database Configuration panel, you can specify that database creation and configuration is to be automated.

    If you do not select the option, you must configure the database manually.
12. On the Remote Access Authorization panel, specify authorization information for the automatic database configuration feature. Specifying the values enables remote configuration.
13. On the Database Administration panel, specify configuration information about the database. The required information varies by database platform.
14. On the Database Tablespace panel, specify information about the table space of the database.

    When you click **Next**, the product installation program connects to the database server and validates the information that you specified.
15. When the database validation is complete, on the Application Server Type panel, specify the application server type for the product deployment.

    You have the option of configuring WebSphere Application Server Network Deployment automatically through the product installation program.
16. On the WebSphereConnectivity panel, specify host information for the WebSphere Application Server Network Deployment.
17. On the WebSphere Remote Access Authorization panel, specify authorization information for WebSphere Application Server Network Deployment configuration.
18. On the WebSphere Application Server Network Deployment Configuration panel, specify configuration information for WebSphere Application Server Network Deployment.

    The web server port must match an existing HTTP server port value that you configured when you set up WebSphere Application Server Network Deployment. If you specify a different value for the web server port, you must restart WebSphere Application Server Network Deployment at the conclusion of the installation. Restarting the server activates the new port and makes it available for incoming requests.

    The application server name that you specify is created if it does not exist.
19. On the Security panel, specify the method to use for authenticating and authorizing users.
20. On the Specify Maximo Users panel, enter Maximo database user information.

    Maximo administration user

    The product administrator user ID that is used for initial configuration and adding users.

    Maximo system registration user

    The user ID that is used for the self-registration of users.

Maximo system integration user
The user ID that is used with enterprise adapters.

Custom user ID and password values are stored in the Maximo database. The default user IDs of maxadmin, maxreg, and maxintadm are also created as users in the Maximo database. Creation of the default user IDs is done for internal processing purposes. If you use Maximo database security for authentication and authorization, the default user IDs can be used to log in to the application. If you regard this condition as a security risk, you can modify the passwords for the default user IDs. You modify passwords for the user IDs in the Users application.

21. On the Security panel, specify the names of the user and group base entries and specify how Maximo Asset Management users are created.

    User base entry
    If you do not plan to use the default LDAP schema that is provided with Maximo Asset Management, specify the user base entry that you want to use.

    Group base entry
    If you do not plan to use the default LDAP schema , specify the group base entry that you want to use.

    You can specify that the installation program creates the required users. Otherwise, you must create users manually before continuing.

    If you are not using the default LDAP schema that is provided, you must create it yourself before advancing beyond this panel. The values that are specified for the **User base entry** and **Group base entry** fields are used to configure the VMMSYNC cron task. To create your own LDAP schema and create users manually, you can modify the default add-on LDIF data and import it into your LDAP repository

22. On the Integration Adapter JMS Configuration panel, specify Java Message Service configuration information. A JMS server requires a DB2 data repository to be configured to maintain messages. If you are using another database type, you cannot configure message persistence. If you specify that JMS messages are not to be persisted, you can configure the JMS implementation manually later.

    Specify the name of the database to be used by JMS. For DB2, you can specify whether to persist JMS messages within DB2.

    Select **Do not persist JMS messages** if you are deploying Maximo Asset Management with Oracle or Microsoft SQL Server. When you click **Next**, the installation wizard skips to the SMTP Configuration panel.

23. On the SMTP Configuration panel, specify the SMTP configuration information that is used by workflows to communicate with workflow participants.

    The administrator e-mail address is the e-mail address that is used to send messages. If you leave the fields blank, you must configure the SMTP parameters through the product interface as a post-installation task.

24. On the Base Language Selection panel, specify the base language for the installation.

25. On the Additional Language Selection panel, you can optionally specify one or more additional languages that the installation is to support.

26. On the Run Configuration Step panel, specify how to perform the configuration step of the installation. If you do not select an option, the configuration step proceeds when you click **Next**.

Copy files now, but perform the installation configuration step later

Select this option to copy files from the installation source to the administrative workstation. You must perform the configuration step at a later time to complete the deployment.

Select this option to create a maxdemo database during the installation of Maximo Asset Management and populate the database with sample data.

Important: Do not install another product before you complete the configuration step of the original installation. Installing another product before you run the configuration step for this installation overwrites the taskstore, which prevents the original installation from ever being deployed.

The configuration values that you specify are stored in the *install_home*\maximo\applications\maximo\properties\maximo.properties and *install_home*\etc\install.properties files. You run the configuration steps outside of the product installation program by using the taskrunner utility, in the *install_home*\scripts directory. Run the taskrunner utility from the command line.

```
install_home\scripts\taskrunner [CONTINUE <STOPONERROR|NOSTOPONERROR>]
```

The taskrunner uses the configuration values that are stored in the `maximo.properties` and `install.properties` files to configure Maximo Asset Management.

If you run taskrunner with the **`NOSTOPONERROR`** parameter, the taskrunner continues despite errors. If you run taskrunner with the **`STOPONERROR`** parameter, the taskrunner stops when it encounters an error. If you used **`STOPONERROR`**, you can rectify the conditions that caused the error. You can then resume the installation where the last successfully completed task was recorded in the previous attempt by starting taskrunner with the **`CONTINUE`** parameter.

Deploy application files manually later

Select this option to manually deploy application files to the application server.

Defer the update of the Maximo database

Select this option if you want to manually run the database update task for the product deployment. This option can be used when there is a fix pack available that addresses known issues with the updatedb script. In this scenario, you choose the **Defer the update of the Maximo database** option, apply the fix pack, and then run the **`updatedb -v1`** command manually.

27. On the Choose Shortcut Folder panel, specify where you want Maximo Asset Management icons created.

    If you select **In the Start Menu** and use Internet Explorer, add the Maximo Asset Management URL to the trusted sites web content zone. Disable the option that requires server verification for all sites in the zone.

    Do not select **In the Quick Launch Bar**. The selection does not create a shortcut in the Quick Launch bar.

28. On the Input Summary panel, review the information that you provided for the product installation program.

    If necessary, use **Previous** to return to previous panels to change values.

29. On the Pre-Installation Summary panel, review the installation information, then click **Install**.

    The installation process begins. You can monitor the progress of the installation by viewing the messages that are shown.
30. On the Installation Completed panel, review any information presented, then click **Done**.

"Restarting middleware on Windows" on page 143
This procedure describes how to restart middleware on Windows, if you must restart any middleware services.

"Restarting middleware on UNIX" on page 144
Middleware services on Linux and AIX platforms occasionally must be restarted, such as when a reboot occurs. Middleware servers and services must be active before running the Maximo Asset Management installation program.

Creating a maxdemo database during installation

You can create a maxdemo database during a Maximo Asset Management installation and populate the database with sample data.

Procedure

1. On the Run Configuration Step panel of the installation wizard, select **Copy files now, but perform the installation configuration later**.
2. When the installation finishes, exit the installation wizard.
3. Rename the `C:\IBM\SMP\Maximo\tools\maximo\en\maximo.`*`dbtype`* file.
4. Copy the `C:\IBM\SMP\Maximo\tools\maximo\en\maxdemo.`*`dbtype`* file to `C:\IBM\SMP\Maximo\tools\maximo\en\maximo.`*`dbtype`*, where `en` is the language folder and the *dbtype* is `ora`, `sqs`, or `db2`.
5. Open a command window and browse to `C:\IBM\SMP\scripts`.
6. Run the following command: `taskrunner.bat CONTINUE STOPONERROR`
7. When the taskrunner process is complete, change the file names back to their original names. Do not restart the computer before you run the taskrunner command. The taskrunner utility does not create a persistent store of information and data can be lost.

Language deployment after database update deferral

Selecting the option to defer the update of the Maximo database when installing the product, affects how you deploy languages.

During installation, you have the option to defer the database update task. This option prevents writing data to the database during the installation. The installation program is limited to copying files to the administrative system and registering product process solution packages. You add languages by completing the installation, manually updating the database, and then updating languages manually.

"Manually deploying languages after database update deferral"
Languages must be deployed manually if you defer database updates by the installation program.

Manually deploying languages after database update deferral

Languages must be deployed manually if you defer database updates by the installation program.

Before you begin

You must have run updatedb command before manually configuring languages for PSI packages.

About this task

To manually configure languages for PSI packages, complete the following steps:

Procedure

Update language support for the Maximo core components.
Files for the language selections you made during the installation are extracted to the `C:\IBM\SMP\Maximo\Tools\Maximo\locale\xliff\` directory on the system.

1. To update a language as the base language to use for the product, run the following command:

   ```
   install_home\maximo\tools\maximo\TDToolkit.bat
   -IMPORT
   -SLEN
   -TLlocale
   -maxmessfix
   ```

2. To add one or more languages as additional languages for use with the product, run the following command for each language you want to add:

   ```
   install_home\maximo\tools\maximo\TDToolkit.bat
   -ADDLANGlocale
   -maxmessfix
   ```

Chapter 3. Deploying automatically reusing existing middleware

Use this information to use Maximo Asset Management installation programs and tools to automatically configure existing middleware within your enterprise during the Maximo Asset Management deployment process.

This information provides a high-level overview or road map of tasks you need to complete in order to deploy Maximo Asset Management automatically. You use middleware already established in your enterprise.

In this scenario, you use the middleware installation program and the Maximo Asset Management installation program to automatically configure existing middleware resources. Middleware configuration is performed automatically before deploying the product.

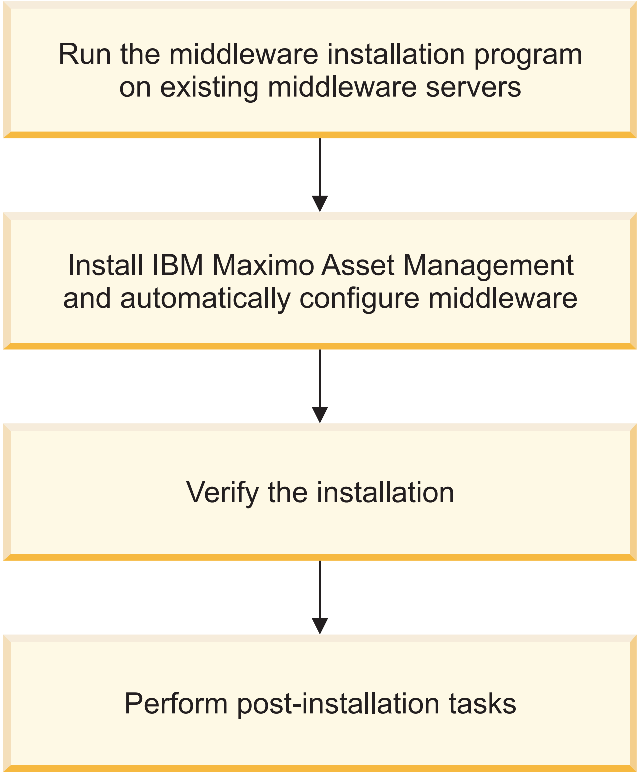
Run the middleware installation program on existing middleware servers
Install IBM Maximo Asset Management and automatically configure middleware
Verify the installation
Perform post-installation tasks

Figure 2. Deploying Maximo Asset Management reusing existing middleware

Run the middleware installation program on existing middleware servers

If you intend to reuse existing middleware servers with Maximo Asset Management, they must be configured before you run the Maximo Asset Management installation program.

Information for using the middleware installation program with IBM Tivoli Directory Server is included.

You cannot use the middleware installation program to configure existing Oracle servers.

The middleware installation program cannot configure an existing WebSphere Application Server Network Deployment deployment.

Ensure that all of your middleware is at supported levels for Maximo Asset Management.

When you install and configure middleware in the middleware installation program and the Maximo Asset Management installation program, consider the following special characters restrictions:

Table 3. Middleware object naming conventions

Naming Convention	Details
IBM Tivoli Directory Server conventions for databases and database aliases.	Database names must be unique within the location in which they are cataloged. For Linux and UNIX , this location is a directory path. For Windows it is a logical disk. Database alias names must be unique within the system database directory. When a new database is created, the alias defaults to the database name. As a result, you cannot create a database using a name that exists as a database alias, even if there is no database with that name. Database and database alias names can have up to 8 characters. Be mindful that the special characters @, #, and $ are not common to all keyboards. Avoid these characters when you create a database name.
IBM Tivoli Directory Server conventions for users, groups, databases, and instances	Values must not be longer than 8 characters. Values cannot be any of the following: USERS, ADMINS, GUESTS, PUBLIC, LOCAL, or idsldap Values cannot begin with IBM, SQL, or SYS. Values must not include accented characters. Values can include characters A through Z, a through z, and 0 through 9. Values must begin with characters A through Z or a through z. Double-byte characters cannot be used in administrator passwords values. Passwords cannot contain the following special characters: ` ' \ " |

Table 3. Middleware object naming conventions (continued)

Naming Convention	Details
WebSphere Application Server Network Deployment conventions	The administrator name cannot contain the following characters: / \ * ,: ;=+? | < > & % '"] [> # $ ~ ( ) The administrator name cannot begin with a period. The administrator name cannot contain leading and trailing spaces. The administrator password must consist of 8 characters.
The middleware installation program	The middleware installation program does not validate that your password is compliant with the operating system of the target host. Ensure that the password values you provide are valid for your environment. The middleware installation program does not allow the use of the '%' character on Windows and the use of the !, $, #, % characters on UNIX. The middleware installation program does not check for accented characters in user name values. The use of accented characters can cause errors.

Verifying an existing IBM Tivoli Directory Server using the middleware installer

If you have an existing IBM Tivoli Directory Server installation that you would like to reuse for Maximo Asset Management, you can verify that it works with Maximo Asset Management using the middleware installer.

About this task

The middleware installer validates the following items:

- The version of IBM Tivoli Directory Server is compatible with Maximo Asset Management.
- The IBM Tivoli Directory Server is running.
- The Base DN information that you supply in the middleware installer panels are present in the IBM Tivoli Directory Server you are using.

  The middleware installer does not create an instance of IBM Tivoli Directory Server for use with Maximo Asset Management. If you want to reuse an existing instance of IBM Tivoli Directory Server, supply the correct Administrator Distinguished Name and password, LDAP BASE DN, directory server port, and the administration port information for that instance on the middleware installer panels when prompted. If you intend to host a new instance on your existing IBM Tivoli Directory Server, you must create it before you run the middleware installer.

  Note: While you can technically share a DB2 instance between Maximo Asset Management and the one required by IBM Tivoli Directory Server, it is not a recommended practice. During the installation, the database instance is restarted, which might disrupt the availability of IBM Tivoli Directory Server in your enterprise. If you are using the automated installers, separate instances are created for use by Maximo Asset Management and IBM Tivoli Directory Server.

To have the middleware installer verify an existing instance of IBM Tivoli Directory Server for reuse with Maximo Asset Management, complete the following steps.

Procedure

1. Log in to the system as a user with administrative authority.
2. Start the middleware installer from the product launchpad.
3. Navigate the middleware installer panels up to the point where you reach the deployment choices panel.
4. In the deployment choices panel, select **Directory Server**, and then click **Next**. The middleware installer displays any instances of IBM Tivoli Directory Server discovered on the system.
5. In the Installation menu, select the appropriate instance to reuse, and then click **Next**.
6. Complete the installation by navigating the rest of the middleware installer panels.

“Manually configuring the directory server” on page 60
These topics provide details on manually configuring a directory server for use by Maximo Asset Management

“Installing middleware using the middleware installation program” on page 18
You use the middleware installation program to install middleware components for use with IBM Maximo Asset Management. The middleware components that you choose to install, and the associated configuration parameters, are recorded in a deployment plan for the target system.

Installation program overview

The Maximo Asset Management installation program provides an interface for installing and deploying Maximo Asset Management, which includes the process automation engine and process managers.

The Maximo Asset Management installation program records choices you make about your Maximo Asset Management deployment. It records configuration parameters associated with those choices, and then installs and deploys Maximo Asset Management based upon the information you entered.

There are two installation paths available to you when you are installing Maximo Asset Management.

Simple

A simple deployment consists of installing Maximo Asset Management middleware on one system. You do not have the option of using existing middleware within your organization with Maximo Asset Management. All middleware used with Maximo Asset Management must be installed on the system with the middleware installation program with default values. Maximo Asset Management is installed with default values provided by the middleware installation program and Maximo Asset Management installation program.

If you intend to override default values used by the simple deployment path, you must use the custom deployment path instead.

Custom

A custom deployment typically involves deploying Maximo Asset Management across several systems. Some of these systems might already host middleware products that you want to use with your Maximo Asset Management deployment. You can modify default installation values when you deploy with the custom installation path.

This deployment option does not require you to spread the Maximo Asset Management deployment across several systems. You can enter the name of the local host as the destination for all Maximo Asset Management components.

The Maximo Asset Management installation program can automate the configuration of some middleware for use with Maximo Asset Management.

If you choose not to have the Maximo Asset Management installation program automatically configure middleware, you must configure that piece of middleware manually **before** the installation of Maximo Asset Management.

Important: When you are entering LDAP values for Maximo Asset Management installation panel fields, be aware of the product-specific syntax rules for using special characters in an LDAP string. In most cases, special characters must be preceded by an escape character in order to make it readable by the directory server. Failing to escape special characters contained in an LDAP string used with Maximo Asset Management results in Maximo Asset Management errors.

Many directory server products consider a blank space as a special character that is part of the LDAP string. If you enter an LDAP string with an unescaped blank character at the end of a field value, you encounter Maximo Asset Management errors.

For more information about special character usage in LDAP strings, see the product documentation for your directory server.

Information that you enter for the Maximo Asset Management installation program is stored in the `maximo.properties` and `install.properties` files and the Maximo database. These values are populated into the panel fields of the Maximo Asset Management installation program on subsequent uses of the program. If you cancel the installation program, it recalls most values that you entered the next time you start it. Values excluded from being saved in this manner are the Maximo Asset Management installation directory and the shortcut option chosen during the installation. You can restore the default values in the Maximo Asset Management installation program by deleting `<`*`Maximo_Home`*`>/applications/maximo/properties/maximo.properties` and `<`*`Maximo_Home`*`>/etc/install.properties`. If you cannot locate the `maximo.properties` file in the `<Maximo_Home>` directory, look for it in the system temp file directory.

Installing the product and automatically configuring middleware

To install Maximo Asset Management, you run the installation program from the launchpad. The installation procedure automatically configures middleware on multiple servers, using default values.

Before you begin

Ensure that you meet prerequisite conditions.

- The database server, the directory server, and application server services must be started and active.
- On the administrative workstation, temporarily shut down any noncritical processes that can have a negative effect on the installation, such as antivirus software.
- Ensure that the Windows DEP setting does not prevent the launchpad from running: Select **Start** > **Settings** > **Control Panel** > **System** > **Advanced** > **Performance** > **Settings** > **Data Execution Prevention**. Select **Turn on DEP for essential Windows programs and services only** and click **Apply**. You might be asked to reboot the server.
- For Linux and UNIX systems with middleware installed, the command **`hostname -f`** must return a fully qualified host name. If necessary, consult the documentation for your operating system. Alternatively, you can provide the IP address for the system.
- Enable a remote execution and access service on every system that has middleware installed. Each remote system must support a remote access protocol. It must also accept remote logins from a user name and password that were configured on the target server. Remote access protocols include SSH and Windows SMB. If the remote system is a Windows server, you must configure remote execution and access to use SMB.

About this task

The instructions are for a multiple server installation that uses default values.

Procedure

1. Log in on the administrative system.
2. Start the product installation program from the launchpad.
   a. Start the launchpad. Browse to the root directory of the downloaded installation image, and run the following command:

      Windows

      ```
      launchpad.exe
      ```

   b. In the launchpad navigation pane, click **Install Product**.

   c. Click **Install Maximo Asset Management 7.5**.

   If the launchpad does not start the installation, you can start the product installation program directly. On the downloaded installation image, browse to `\Install\mam\`, and run one of the following commands:

   Windows

   - `install.bat`
   - `install_win64.bat`
3. Select a language for the installation and click **OK**.
4. On the Choose Installation Folder panel, specify the path to the location where you want to install Maximo Asset Management.

   You can specify a description for the installation. A description is useful for differentiating between multiple installations that are hosted on the same administrative workstation.
5. Review the information that is on the Verify Installation Location panel. The panel shows any previous installation information that was found based on the installation directory that you specified on the previous panel. After you advance past this panel, you cannot go back and change the installation directory for this installation.

If a more recent version of the installation program is found in the specified target directory, you are notified. The notification means that you are using an older version of the installation program. The version found on the administrative workstation is newer and can contain important features and enhancements. To use the newer version of the installation program, select the option on the notification panel and click **Next**. This action exits the current installation process and restarts the installation process with the newer installation program. If you do not select the option, you continue the installation with the older version of the installation program.

6. On the Package Summary panel, review the package deployment information. This panel lists version information for both new and existing packages on the system. Target package version information indicates the package version being currently deployed.
7. On the Choose Deployment panel, specify **Simple** or **Custom** as the deployment type.
8. On the Import Middleware Configuration Information panel, you select **Import middleware configuration information** to have the product installation program reuse the middleware installation program values. These values are used as default values for the same fields in the product installation program.

   The **Workspace location** field refers to the location of the topology file that contains the values that were specified for the middleware installation program. The file is located in the workspace that was defined during the middleware installation task. For example, `C:\ibm\tivoli\mwi\workspace` for Windows or `/root/ibm/tivoli/mwi/workspace` for UNIX.

   If you selected the simple deployment, the middleware default information is not used.
9. On the Database Type panel, specify the software to use for the Maximo database.
10. On the Database panel, specify configuration information for your database software.

    For things such as the database user ID, the database name, the database instance for Maximo Asset Management, and the schema name, if the values do not exist when you specify them, they are created.

    Database users and database instance names cannot contain spaces.

    After you specify configuration information for your database software, the installation program validates the information with the database server.
11. On the Automate Database Configuration panel, you can specify that database creation and configuration is to be automated.

    If you do not select the option, you must configure the database manually.
12. On the Remote Access Authorization panel, specify authorization information for the automatic database configuration feature. Specifying the values enables remote configuration.
13. On the Database Administration panel, specify configuration information about the database. The required information varies by database platform.
14. On the Database Tablespace panel, specify information about the table space of the database.

    When you click **Next**, the product installation program connects to the database server and validates the information that you specified.
15. When the database validation is complete, on the Application Server Type panel, specify the application server type for the product deployment.

You have the option of configuring WebSphere Application Server Network Deployment automatically through the product installation program.

16. On the WebSphereConnectivity panel, specify host information for the WebSphere Application Server Network Deployment.
17. On the WebSphere Remote Access Authorization panel, specify authorization information for WebSphere Application Server Network Deployment configuration.
18. On the WebSphere Application Server Network Deployment Configuration panel, specify configuration information for WebSphere Application Server Network Deployment.

    The web server port must match an existing HTTP server port value that you configured when you set up WebSphere Application Server Network Deployment. If you specify a different value for the web server port, you must restart WebSphere Application Server Network Deployment at the conclusion of the installation. Restarting the server activates the new port and makes it available for incoming requests.

    The application server name that you specify is created if it does not exist.
19. On the Security panel, specify the method to use for authenticating and authorizing users.
20. On the Specify Maximo Users panel, enter Maximo database user information.

    Maximo administration user

    The product administrator user ID that is used for initial configuration and adding users.

    Maximo system registration user

    The user ID that is used for the self-registration of users.

    Maximo system integration user

    The user ID that is used with enterprise adapters.

    Custom user ID and password values are stored in the Maximo database. The default user IDs of maxadmin, maxreg, and maxintadm are also created as users in the Maximo database. Creation of the default user IDs is done for internal processing purposes. If you use Maximo database security for authentication and authorization, the default user IDs can be used to log in to the application. If you regard this condition as a security risk, you can modify the passwords for the default user IDs. You modify passwords for the user IDs in the Users application.
21. On the Security panel, specify the names of the user and group base entries and specify how Maximo Asset Management users are created.

    User base entry

    If you do not plan to use the default LDAP schema that is provided with Maximo Asset Management, specify the user base entry that you want to use.

    Group base entry

    If you do not plan to use the default LDAP schema , specify the group base entry that you want to use.

    You can specify that the installation program creates the required users. Otherwise, you must create users manually before continuing.

    If you are not using the default LDAP schema that is provided, you must create it yourself before advancing beyond this panel. The values that are specified for the **User base entry** and **Group base entry** fields are used to configure the VMMSYNC cron task. To create your own LDAP schema and create users manually, you can modify the default add-on LDIF data and import it into your LDAP repository

22. On the Integration Adapter JMS Configuration panel, specify Java Message Service configuration information. A JMS server requires a DB2 data repository to be configured to maintain messages. If you are using another database type, you cannot configure message persistence. If you specify that JMS messages are not to be persisted, you can configure the JMS implementation manually later.

    Specify the name of the database to be used by JMS. For DB2, you can specify whether to persist JMS messages within DB2.

    Select **Do not persist JMS messages** if you are deploying Maximo Asset Management with Oracle or Microsoft SQL Server. When you click **Next**, the installation wizard skips to the SMTP Configuration panel.

23. On the SMTP Configuration panel, specify the SMTP configuration information that is used by workflows to communicate with workflow participants.

    The administrator e-mail address is the e-mail address that is used to send messages. If you leave the fields blank, you must configure the SMTP parameters through the product interface as a post-installation task.

24. On the Base Language Selection panel, specify the base language for the installation.

25. On the Additional Language Selection panel, you can optionally specify one or more additional languages that the installation is to support.

26. On the Run Configuration Step panel, specify how to perform the configuration step of the installation. If you do not select an option, the configuration step proceeds when you click **Next**.

    Copy files now, but perform the installation configuration step later

    Select this option to copy files from the installation source to the administrative workstation. You must perform the configuration step at a later time to complete the deployment.

    Select this option to create a maxdemo database during the installation of Maximo Asset Management and populate the database with sample data.

    Important: Do not install another product before you complete the configuration step of the original installation. Installing another product before you run the configuration step for this installation overwrites the taskstore, which prevents the original installation from ever being deployed.

    The configuration values that you specify are stored in the `*install_home*\maximo\applications\maximo\properties\maximo.properties` and `*install_home*\etc\install.properties` files. You run the configuration steps outside of the product installation program by using the taskrunner utility, in the `*install_home*\scripts` directory. Run the taskrunner utility from the command line.

    ```
    install_home\scripts\taskrunner [CONTINUE <STOPONERROR|NOSTOPONERROR>]
    ```

    The taskrunner uses the configuration values that are stored in the `maximo.properties` and `install.properties` files to configure Maximo Asset Management.

If you run taskrunner with the `NOSTOPONERROR` parameter, the taskrunner continues despite errors. If you run taskrunner with the `STOPONERROR` parameter, the taskrunner stops when it encounters an error. If you used `STOPONERROR`, you can rectify the conditions that caused the error. You can then resume the installation where the last successfully completed task was recorded in the previous attempt by starting taskrunner with the `CONTINUE` parameter.

Deploy application files manually later
Select this option to manually deploy application files to the application server.

Defer the update of the Maximo database
Select this option if you want to manually run the database update task for the product deployment. This option can be used when there is a fix pack available that addresses known issues with the updatedb script. In this scenario, you choose the **Defer the update of the Maximo database** option, apply the fix pack, and then run the **`updatedb -v1`** command manually.

27. On the Choose Shortcut Folder panel, specify where you want Maximo Asset Management icons created.

    If you select **In the Start Menu** and use Internet Explorer, add the Maximo Asset Management URL to the trusted sites web content zone. Disable the option that requires server verification for all sites in the zone.

    Do not select **In the Quick Launch Bar**. The selection does not create a shortcut in the Quick Launch bar.
28. On the Input Summary panel, review the information that you provided for the product installation program.

    If necessary, use **Previous** to return to previous panels to change values.
29. On the Pre-Installation Summary panel, review the installation information, then click **Install**.

    The installation process begins. You can monitor the progress of the installation by viewing the messages that are shown.
30. On the Installation Completed panel, review any information presented, then click **Done**.

"Restarting middleware on Windows" on page 143
This procedure describes how to restart middleware on Windows, if you must restart any middleware services.

"Restarting middleware on UNIX" on page 144
Middleware services on Linux and AIX platforms occasionally must be restarted, such as when a reboot occurs. Middleware servers and services must be active before running the Maximo Asset Management installation program.

Creating a maxdemo database during installation

You can create a maxdemo database during a Maximo Asset Management installation and populate the database with sample data.

Procedure

1. On the Run Configuration Step panel of the installation wizard, select **Copy files now, but perform the installation configuration later**.
2. When the installation finishes, exit the installation wizard.
3. Rename the `C:\IBM\SMP\Maximo\tools\maximo\en\maximo.`*`dbtype`* file.

4. Copy the `C:\IBM\SMP\Maximo\tools\maximo\en\maxdemo.`*`dbtype`* file to `C:\IBM\SMP\Maximo\tools\maximo\en\maximo.`*`dbtype`*, where `en` is the language folder and the *dbtype* is `ora`, `sqs`, or `db2`.
5. Open a command window and browse to `C:\IBM\SMP\scripts`.
6. Run the following command: `taskrunner.bat CONTINUE STOPONERROR`
7. When the taskrunner process is complete, change the file names back to their original names. Do not restart the computer before you run the taskrunner command. The taskrunner utility does not create a persistent store of information and data can be lost.

Language deployment after database update deferral

Selecting the option to defer the update of the Maximo database when installing the product, affects how you deploy languages.

During installation, you have the option to defer the database update task. This option prevents writing data to the database during the installation. The installation program is limited to copying files to the administrative system and registering product process solution packages. You add languages by completing the installation, manually updating the database, and then updating languages manually.

“Manually deploying languages after database update deferral” on page 38
Languages must be deployed manually if you defer database updates by the installation program.

Manually deploying languages after database update deferral

Languages must be deployed manually if you defer database updates by the installation program.

Before you begin

You must have run updatedb command before manually configuring languages for PSI packages.

About this task

To manually configure languages for PSI packages, complete the following steps:

Procedure

Update language support for the Maximo core components.
Files for the language selections you made during the installation are extracted to the `C:\IBM\SMP\Maximo\Tools\Maximo\`*`locale`*`\xliff\` directory on the system.

1. To update a language as the base language to use for the product, run the following command:

   ```
   install_home\maximo\tools\maximo\TDToolkit.bat
   -IMPORT
   -SLEN
   -TLlocale
   -maxmessfix
   ```

2. To add one or more languages as additional languages for use with the product, run the following command for each language you want to add:

   ```
   install_home\maximo\tools\maximo\TDToolkit.bat
   -ADDLANGlocale
   -maxmessfix
   ```

Chapter 4. Deploying manually reusing existing middleware

Use this information if you intend to deploy Maximo Asset Management by reusing existing middleware servers and manually configuring them to work with Maximo Asset Management.

This information provides a high-level overview or road map of tasks you need to complete in order to deploy Maximo Asset Management automatically, using middleware already established in your enterprise.

In this scenario, you manually configure existing middleware resources before running the Maximo Asset Management installation program.

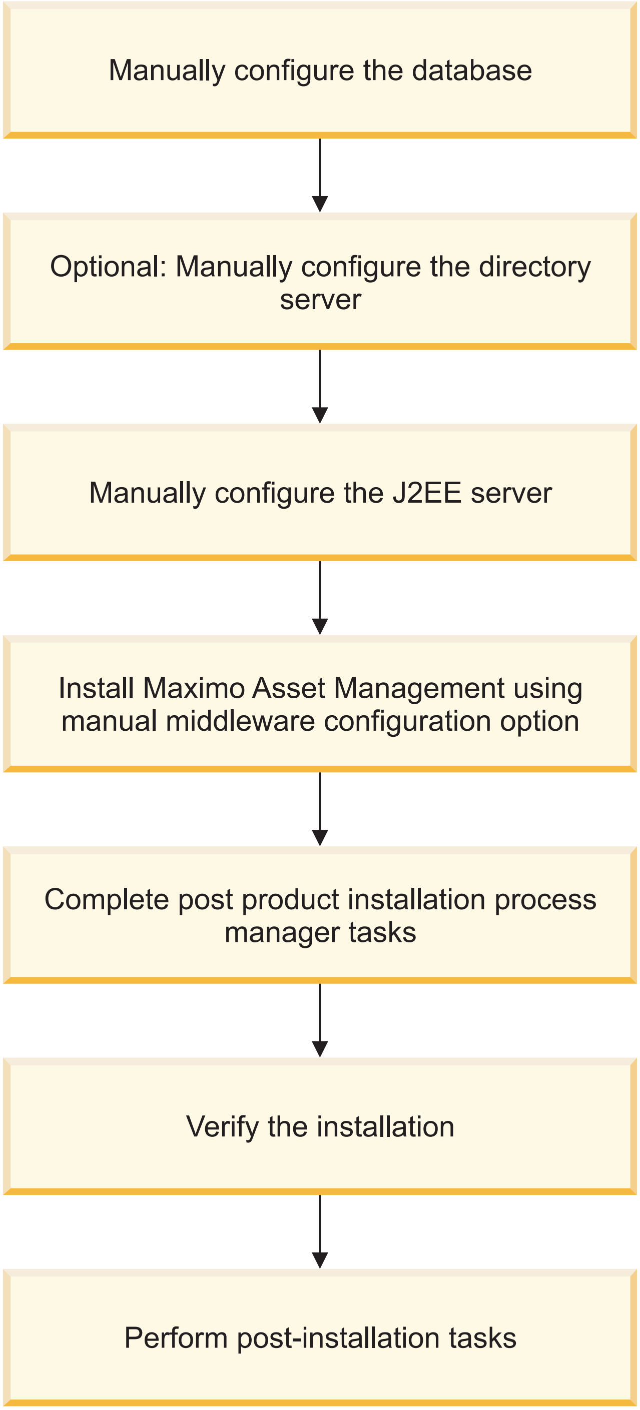
Manually configure the database
Optional: Manually configure the directory server
Manually configure the J2EE server
Install Maximo Asset Management using manual middleware configuration option
Complete post product installation process manager tasks
Verify the installation
Perform post-installation tasks

Figure 3. Deploying Maximo Asset Management with manual middleware configuration

Maximo Asset Management installation with manual middleware configuration

Manually configured installations involve configuring middleware components, the database server, the directory server, and the J2EE server, to work with Maximo Asset Management before using the Maximo Asset Management installation program.

You can elect to have one or more Maximo Asset Management middleware components configured automatically by the Maximo Asset Management installation program. Alternatively, you can choose to manually configure one or more of the middleware servers to work with Maximo Asset Management.

The information contained in this section provides details on how to manually configure Maximo Asset Management middleware before running the Maximo Asset Management installation program.

Before you begin, ensure you have addressed the following prerequisite conditions:

- You have designated a Windows or UNIX-based server to start the Maximo Asset Management installation program.
- For WebSphere Application Server Network Deployment, ensure that the Cell and all related nodes are active.

You must complete the manual configuration of each server you plan to not configure using the autoconfigure feature of the Maximo Asset Management installation program before you actually use the Maximo Asset Management installation program to install Maximo Asset Management.

Ensure that all of your middleware is at supported version levels.

Manually configuring the database

You have the option of manually configuring the database server used in Maximo Asset Management deployment. Manual configuration of the database server must be completed before you use the Maximo Asset Management installation program.

Manually configuring Oracle 11g

Use the following instructions to manually configure Oracle 11g for use with Maximo Asset Management.

Before you begin

Oracle instance names must be limited to eight characters in length. For Oracle databases, the schema owner must use the same user ID as the database user.

About this task

To configure an existing Oracle 11g server for use with Maximo Asset Management, complete the following steps before you start the Maximo Asset Management installation program:

Procedure

1. Log in as the Oracle software user. Typically this user is named `oracle`.

2. Create the database listener. The listener manages requests to connect to the database. This step is only required if you do not already have an existing listener in place.
   a. Open the Oracle Network Configuration Assistant application.
   b. From the Welcome panel, select **Listener configuration**, and then click **Next**.
   c. From the action panel, select **Add**, and then click **Next**.
   d. Enter a name for the listener or accept the default value, and then click **Next**.
   e. Accept the default Selected Protocols listed by clicking **Next**.
   f. From the port panel, select **Use the standard port of 1521**, and then click **Next**.
   g. Select **No** to indicate that you are finished configuring listeners, and then click **Next**.
   h. From the Listener Configuration Done panel, click **Next**.
   i. Click **Finish**.
3. Create a database for use by Maximo Asset Management.
   a. Open the Oracle Database Configuration Assistant.
   b. Click **Next**.
   c. Select **Create a Database**, and then click **Next**.
   d. Select **General Purpose or Transaction Processing**, and then click **Next**.
   e. Enter `ctginst1` for both the Global Database Name value and the SID value, and then click **Next**.
   f. Leave the defaults selected, and click **Next**.
   g. Ensure **Use the Same Administrative Password for All Accounts** is selected, enter a password for Oracle users, and then click **Next**.
   h. Ensure **File System** is selected as the storage mechanism to use for the database. Ensure **Use Database File Locations from Template** is selected as the value to use for database file location, and then click **Next**.
   i. Leave defaults selected for the database recovery options panel, and then click **Next**.
   j. From the Sample Schemas panel, click **Next**.
   k. From the Initialization Parameters panel, on the Memory tab, select **Custom** and provide the following values (measured in Mb):

      Memory Management
      Set this value to **Manual Shared Memory Management**.

      Shared Pool
      Set this value to `152`.

      Buffer Cache
      Set this value to `36`.

      Java Pool
      Set this value to `32`.

      Large Pool
      Set this value to `8`.

      PGA Size
      Set this value to `36`.
   l. From the Character Sets tab, select **Use Unicode (AL32UTF8)**.
   m. Click **All Initialization Parameters...**.

n. Click **Show Advanced Parameters**.

o. Locate the following parameters, change them to the values indicated, and then click **Close**.

   nls_length_semantics
   Change this value to **CHAR**.

   open_cursors
   Change this value to 1000.

   cursor_sharing
   Set this value to FORCE.

p. From the Initialization Parameters panel, click **Next**.

q. From the Database Storage panel, click **Next**.

r. From the Creation Options panel, click **Finish**.

s. Click **Exit** to exit the Database Configuration Assistant. The database is successfully created.

Note: The Oracle Database Configuration Assistant starts the ORACLE_HOME/ctx/admin/defaults/drdefus.sql script as part of the configuration of the CTXSYS user. You must start this script manually if the Oracle Database Configuration Assistant is not used.

4. Create a table space using the following command in SQL*Plus:

```
Create tablespace maxdata datafile
'C:\oracle\product\11.1.0\db_1\dbs\maxdata.dbf'
size 1000M autoextend on;
```

   Change the directory specified in the example to the database location. If the directory does not exist, this command fails.

5. Create a temporary table space using the following command in SQL*Plus

```
create temporary tablespace maxtemp tempfile
'C:\oracle\product\11.1.0\db_1\dbs\maxtemp.dbf'
size 1000M autoextend on maxsize unlimited;
```

   Change the directory specified in the example to the database location. If the directory does not exist, this command fails.

6. Create the maximo user and grant permissions using the following command in SQL*Plus:

```
create user maximo identified by maximo default tablespace maxdata temporary
tablespace maxtemp;
grant connect to maximo;
grant create job to maximo;
grant create trigger to maximo;
grant create session to maximo;
grant create sequence to maximo;
grant create synonym to maximo;
grant create table to maximo;
grant create view to maximo;
grant create procedure to maximo;
grant alter session to maximo;
grant execute on ctxsys.ctx_ddl to maximo;
alter user maximo quota unlimited on maxdata;
```

   If you created a separate table space for indexing, you must also grant access to that index table space to the maximo user. For example, use the following command if you created a separate table space for indexing called TSI_MAM_OWN.":

```
alter user maximo quota unlimited on TSI_MAM_OWN
```

   These instructions assume that you did not modify default role sets assigned to the Oracle DBA user or user IDs created to connect to the database. If you restricted the default privileges granted to user IDs, you must explicitly grant them to the maximo user. For example, if you do not grant a role such as the select_catalog_role role, you must explicitly grant that role to the maximo user. This assignment can be done by running this SQL*Plus command:

```
grant select_catalog_role to maximo
```

Manually configuring Oracle 10g

Oracle 10g can be manually configured for use with Maximo Asset Management.

Before you begin

Oracle instance names must be limited to eight characters in length. For Oracle databases, the schema owner must use the same user ID as the database user.

About this task

To configure an existing Oracle 10g server for use with Maximo Asset Management, complete the following steps before you start the Maximo Asset Management installation program:

Procedure

1. Log in as the Oracle software user. Typically this user is named `oracle`.
2. Create the database listener. The listener manages requests to connect to the database.
   a. Open the Oracle Network Configuration Assistant application.
   b. From the Welcome panel, select **Listener configuration**, and then click **Next**.
   c. From the action panel, select **Add**, and then click **Next**.
   d. Enter a name for the listener or accept the default value, and then click **Next**.
   e. Accept the default Selected Protocols listed by clicking **Next**.
   f. From the port panel, select **Use the standard port of 1521**, and then click **Next**.
   g. Select **No** to indicate that you are finished configuring listeners, and then click **Next**.
   h. From the Listener Configuration Done panel, click **Next**.
   i. Click **Finish**.
3. Create a database for Maximo Asset Management.
   a. Open the Oracle Database Configuration Assistant.
   b. Click **Next**.
   c. Select **Create a Database**, and then click **Next**.
   d. Select **General Purpose**, and then click **Next**.
   e. Enter `ctginst1` for both the Global Database Name value and the SID value, and then click **Next**.
   f. Leave the defaults selected, and click **Next**.
   g. Ensure **Use the Same Password for All Accounts** is selected, enter a password for Oracle users, and then click **Next**
   h. Ensure **File System** is selected as the storage mechanism to use for the database, and then click **Next**.
   i. Ensure **Use Database File Locations from Template** is selected as the value to use for database file location, and then click **Next**.

j. Leave defaults selected for the database recovery options panel, and then click **Next**.

k. From the Sample Schemas panel, click **Next**.

l. From the memory allocation panel, select **Custom**, provide the following values (measured in bytes), and then click **Next**.

   Shared Memory Management
   Set this value to **Manual**.

   Shared Pool
   Set this value to `152`.

   Buffer Cache
   Set this value to `36`.

   Java Pool
   Set this value to `32`

   Large Pool
   Set this value to `8`.

   PGA Size
   Set this value to `36`.

m. From the Character Sets tab, select **Use Unicode (AL32UTF8),**

n. Click **All Initialization Parameters....**

o. Click **Show Advanced Parameters**.

p. Locate the following parameters, change them to the values indicated, and then click **Close**.

   nls_length_semantics
   Change this value to **CHAR**

   open_cursors
   Change this value to `1000`

   cursor_sharing
   Set this value to `FORCE`.

q. From the Initialization Parameters panel, click **Next**.

r. From the Database Storage panel, click **Next**.

s. From the Creation Options panel, click **Finish**.

t. After the database is created, click **Password Management**.

u. Unlock the CTXSYS account by clearing the check mark in the **Lock Account?** column for that entry, enter a password for the account, and then click **OK**.

v. Click **Exit** to exit the Database Configuration Assistant. The database is successfully created.

Note: The Oracle Database Configuration Assistant uses the `ORACLE_HOME/ctx/admin/defaults/drdefus.sql` script as part of the configuration of the CTXSYS user. This script must be used manually if the Oracle Database Configuration Assistant is not used.

4. Create a table space using the following command in SQL*Plus:

```
Create tablespace maxdata datafile
'C:\oracle\product\10.2.0\oradata\ctginst1\maxdata.dbf'
size 1000M autoextend on;
```

The directory specified in the example must be changed to the installation location of the database. If the directory does not exist, this command fails.

5. Create a temporary table space.
6. Create the maximo user and grant permissions using the following command in SQL*Plus:

   ```
   create user maximo identified by maximo default tablespace maxdata temporary
   tablespace maxtemp;
   grant connect to maximo;
   grant create job to maximo;
   grant create trigger to maximo;
   grant create session to maximo;
   grant create sequence to maximo;
   grant create synonym to maximo;
   grant create table to maximo;
   grant create view to maximo;
   grant create procedure to maximo;
   grant alter session to maximo;
   grant execute on ctxsys.ctx_ddl to maximo;
   alter user maximo quota unlimited on maxdata;
   ```

   If you have elected to create a separate table space for indexing, you must also grant the maximo user access to that index table space. For example, you must perform the following additional SQL*plus command if you had created a separate table space for indexing called TSI_CMDB_OWN:

   ```
   alter user maximo quota unlimited on TSI_CMDB_OWN
   ```

   These instructions assume that you did not modify the default role sets that are assigned to the Oracle DBA user or other database connection user IDs. If you restrict the default privileges granted to user IDs, you must explicitly grant them to the maximo user. For example, the select_catalog_role role is required for user IDs connecting to the database. To deploy Maximo Asset Management successfully, you must explicitly grant that role to the maximo user by using the SQL*Plus command:

   ```
   grant select_catalog_role to maximo
   ```

Manually configuring the directory server

These topics provide details on manually configuring a directory server for use by Maximo Asset Management

There are several methods you can use to secure Maximo Asset Management.If want to use a directory server to secure Maximo Asset Management, you must complete the manual configuration of the directory server before you use the Maximo Asset Management installation program. Manual configuration is necessary if you choose to not have the Maximo Asset Management installation program perform configuration.

Note: The base dn, bind user, and other various node values listed in these sections are defaults. These values are replaced with values applicable to existing LDAP hierarchies within your organization.

Important: When entering LDAP values for Maximo Asset Management installation panel fields, entries in LDIF files, or values you enter directly into a directory instance using directory server tools, be aware of the product-specific syntax rules for using special characters in an LDAP string. In most cases, special characters must be preceded by an escape character in order to make it readable by the directory server. Failing to escape special characters contained in an LDAP string used with Maximo Asset Management results in Maximo Asset Management errors.

Many directory server products consider a blank space as a special character that is part of the LDAP string. If you mistakenly enter an LDAP string that contains a blank, at the end of a field value, for example, and you do not precede the blank character with an escape character, you encounter Maximo Asset Management errors that are difficult to troubleshoot.

See the product documentation for your directory server for more information about special characters in LDAP strings.

Manually configuring IBM Tivoli Directory Server

Use the following instructions to manually configure IBM Tivoli Directory Server for use with Maximo Asset Management.

About this task

To configure IBM Tivoli Directory Server before starting the Maximo Asset Management installation program, you must create an instance of IBM Tivoli Directory Server.

Note: While you can technically share a DB2 instance between Maximo Asset Management and the one needed by IBM Tivoli Directory Server, it might lead to problems. During the installation, the database instance is restarted, which might disrupt the availability of IBM Tivoli Directory Server to your enterprise. If you are using the automated installation programs, separate instances are created for use by Maximo Asset Management and IBM Tivoli Directory Server.

Procedure

1. Using your preferred method, create a user on the system and assign it to the appropriate group.

   Windows
   Create the user `db2admin` and make it a member of the following groups:
   - Windows Administrators
   - DB2ADMNS
   - DB2USERS

   UNIX Create the user `idsccmdb` and make it a member of the following groups:
   - dasadmn1
   - idsldap
   - dbsysadm

   The root user must also be a member of the dasadm1, idsldap, and dbsysadm groups.
2. If the Instance Administration tool is not already started, ensure that you are logged in as an administrator on the system, and then start the tool

   Windows
   Select **Programs** > **IBM Tivoli Directory Server 6.3** > **Instance Administration Tool**.

   UNIX Type **`./opt/IBM/ldap/V6.3/sbin/idsxinst`** at the command line.
3. In the Instance Administration tool, click **Create an instance**.
4. In the Create a new instance window, click **Create a new directory server instance**, and then click **Next**.

5. From the Instance details window, enter values for the following fields, and then click **Next**.

   User name
   Select `idsccmdb` as the system user ID of the user who owns the instance. This name is also the name of the instance.

   Install location
   Enter the location where the instance files are stored.

   Encryption seed string
   Type a string of characters that are used as an encryption seed. This value must be a minimum of 12 characters.

   Instance description
   Enter a brief description of the instance.
6. In the DB2 instance details panel, enter `idsccmdb` as the value for the DB2 instance name field, and then click **Next**.
7. In the TCP/IP settings for multihomed hosts panel, select Listen on all configured IP addresses, and then click **Next**.
8. In the TCP/IP port settings panel, complete the following fields, and then click **Next**.

   Server port number
   Enter `389` as the contact port for the server.

   Server secure port number
   Enter `636` as the secure port for the server.

   Admin daemon port number
   Enter `3538` as the administration daemon port.

   Admin daemon secure port number
   Enter `3539` as the administration daemon secure port.
9. In the Option steps panel, leave the following options selected, and then click **Next**.

   Configure admin DN and password
   You want to configure the administrator DN and password for the instance now.

   Configure database
   You want to configure the database for the directory server now.
10. In the Configure administrator DN and password window panel, complete the following fields, and then click **Next**.

    Administrator DN
    Enter `cn=root` for the administrator distinguished name.

    Administrator Password
    Enter a password for the Administrator DN.
11. From the Configure database panel, complete the following fields, and then click **Next**.

    Database user name
    Enter `idsccmdb` as the database user.

    Password
    Enter the password for the idsccmdb user.

    Database name
    Enter `idsccmdb` as the database to be used with this directory instance.

12. In the Database options panel, complete the following fields, and then click **Next**.

    Database install location

    Type the location for the database.

    Windows

    For Windows platforms, this value must be a drive letter.

    UNIX For non-Windows platforms, the location must be a directory name, such as `/home/ldapdb`.

    Ensure that you have at least 80 MB of free hard disk space in the location you specify. Additional disk space must be available to accommodate growth as new entries are added to the directory.

    Character-set option

    Leave the **Create a universal DB2 database (UTF-8/UCS-2)** option selected.

13. In the Verify settings panel, review the instance creation details provided, and then click **Finish** to create the idsccmdb instance.
14. Click **Close** to close the window and return to the main window of the Instance Administration tool.
15. Click **Close** to exit the Instance Administration tool.
16. Start the IBM Tivoli Directory Server Configuration tool:

    Windows

    Select**Programs** > **IBM Tivoli Directory Server 6.3** > **Instance Administration Tool**.

    UNIX Type **`./opt/IBM/ldap/V6.3/sbin/idsxcfg`** at the command line.

17. Select **Manage suffixes**.
18. In the Manage suffixes panel, type the following suffix, and then click **Add**.

    ```
    o=IBM,c=US
    ```

19. Click **OK**.
20. Create and save an LDIF file.

    Add the DN information, for example:

    - ou=SWG,o=IBM,c=US
    - ou=users

    Note: ou=SWG,o=IBM,c=US in this example is an organization unit called SWG. SWG houses the OU=Users organization units to place the users created for Maximo Asset Management. DC=IBM and DC=COM would indicate a domain forest of ibm.com®. You can replace the example with the directory structure of your own organization.
    Define the following users and their positions within the ou=users DN's you created. These users are defined in order for Virtual Member Manager to be used to secure Maximo Asset Management.

    Important: Before you begin this procedure, ensure that you have the following users created in the root of your LDAP repository:

Table 4. Base Maximo Asset Management required users

User
wasadmin
maxadmin

Table 4. Base Maximo Asset Management required users (continued)

User
mxintadm
maxreg

Here is an example of the default base LDIF data:

```
dn: o=ibm,c=us
objectClass: top
objectClass: organization
o: IBM

dn: ou=SWG, o=ibm,c=us
ou: SWG
objectClass: top
objectClass: organizationalUnit

dn: ou=users,ou=SWG, o=ibm,c=us
ou: users
objectClass: top
objectClass: organizationalUnit
dn: cn=wasadmin,ou=users,ou=SWG, o=ibm,c=us
uid: wasadmin
userpassword: wasadmin
objectclass: organizationalPerson
objectclass: inetOrgPerson
objectclass: person
objectclass: top
title: WebSphere Administrator
sn: wasadmin
cn: wasadmin
dn: uid=maxadmin,ou=users,ou=SWG, o=ibm,c=us
userPassword: maxadmin
uid: maxadmin
objectClass: inetorgperson
objectClass: top
objectClass: person
objectClass: organizationalPerson
sn: maxadmin
cn: maxadmin

dn: uid=mxintadm,ou=users,ou=SWG, o=ibm,c=us
userPassword: mxintadm
uid: mxintadm
objectClass: inetorgperson
objectClass: top
objectClass: person
objectClass: organizationalPerson
sn: mxintadm
cn: mxintadm

dn: uid=maxreg,ou=users,ou=SWG, o=ibm,c=us
userPassword: maxreg
uid: maxreg
objectClass: inetorgperson
objectClass: top
objectClass: person
objectClass: organizationalPerson
sn: maxreg
cn: maxreg
```

Note: If you create the LDIF file on Windows, ensure that you remove the ^M characters from the file before using.

Note: Before you can import an LDIF file on UNIX systems, you must run the dos2unix command to format the file.

21. In the IBM Tivoli Directory Server Configuration Tool, click **Import LDIF data**.
22. Click **Browse** to locate the LDIF file.
23. Click **Import**.
24. Close the IBM Tivoli Directory Server Configuration Tool and restart the server.

Manually configuring the J2EE server

This section contains instructions for manually configuring an existing J2EE server for use by Maximo Asset Management.

Manual configuration of the J2EE server is required if you choose to deploy Maximo Asset ManagementWebSphere Application Server Network Deployment and you choose to not have the Maximo Asset Management installation program automatically configure it. You must complete the manual configuration before you use the Maximo Asset Management installation program.

Manually configuring WebSphere Application Server Network Deployment

This section contains instructions for manually configuring an existing WebSphere Application Server Network Deployment for use by Maximo Asset Management.

You must manually configure WebSphere Application Server Network Deployment before you use the Maximo Asset Management installation program if you do not want the Maximo Asset Management installation program to configure it automatically.

Performing WebSphere Application Server Network Deployment configuration tasks:

Use this procedure to perform WebSphere Application Server Network Deployment configuration tasks.

About this task

If you elect to manually configure Maximo Asset Management middleware for use with Maximo Asset Management, you have to manually configure the WebSphere Application Server Network Deployment.

Procedure

1. Manually copy the keystore file from the WebSphere Application Server Network Deployment deployment manager host to a temporary directory on the Maximo Asset Management administrative system where you are installing Maximo Asset Management: `*WAS_HOME*/profiles/ctgDmgr01/etc/trust.p12`
2. Open a browser and access the administrative console by typing in the browser address bar: `http://*server_name*:9060/admin`. This URL address depicts the default port number (9060) and context (admin) for the administrative console. Enter a user name to log in. The browser is redirected to a secure port (9043).
3. Create the MXServer application server. This step is only necessary if you did not install WebSphere Application Server Network Deployment v7 using the

middleware installation program. For WebSphere Application Server Network Deployment v8, you must create the application server.

a. Expand **Servers** > **Server Types** > **WebSphere application servers**.

b. Click **New**.

c. Type `MXServer` and click **Next**.

d. Accept all default settings and click **Next**.

e. Accept default settings and click **Next**.

f. Click **Finish**.

g. Click **Preferences**.

h. Select the **Synchronize changes with Nodes** check box, and then click **Apply**.

i. Click **Save**.

j. Click **OK**.

4. Edit JVM Memory Settings and JVM Arguments for the application server.

   a. Click **MXServer** in the main window.

   b. From the Server Infrastructure group, expand the **Java and Process Management** link.

   c. Click **Process Definition**.

   d. Click **Java Virtual Machine**.

   e. For 32-bit platforms, scroll down and type `1536` for **Initial Heap Size** and **Maximum Heap Size**. For 64-bit platforms, set these values to `4096`.

   f. Enter the following values in the **Generic JVM arguments** field, using a space between each argument:

   ```
   -Dsun.rmi.dgc.ackTimeout=1000
   -Xdisableexplicitgc
   -Xgcpolicy:gencon
   -Xmn320m     # 320 for 32-bit JVM, 1024 for 64-bit JVM
   -Xlp64k      # AIX
   ```

   g. Click **OK**.

   h. Click **Save** in the messages box.

5. Edit thread pool settings for the application server.

   a. Click **MXServer** from the **WebSphere application servers** panel.

   b. From the Additional Properties group, click **Thread pools**.

   c. Click **Default**. Set **Minimum Size** to `20`. Set **Maximum Size** to `50`. Set **Thread inactivity timeout** to `30000`. Click **OK**.

   d. Click **TCPChannel.DCS**. Set **Minimum Size** to `5`. Set **Maximum Size** to `20`. Set **Thread inactivity timeout** to `5000`. Click **OK**.

   e. Click **WebContainer**. Set **Minimum Size** to `20`. Set **Maximum Size** to `50`. Set **Thread inactivity timeout** to `30000`. Click **OK**.

6. Edit JVM Memory Settings for the deployment manager.

   a. From **System administration**, click **Deployment manager**.

   b. From the Server Infrastructure group, expand the **Java and Process Management** link.

   c. Click **Process Definition**.

   d. Click **Java Virtual Machine**.

   e. Scroll down and type `512` for Initial Heap Size and `1024` for Maximum Heap Size and click **OK**.

   f. Click **Save** in the messages box.

7. Start the application server.
   a. From **Servers** > **Server Types** > **WebSphere application servers**, click **Application servers**.
   b. Select the check box beside MXServer.
   c. Click **Start**.
8. Identify the HTTP Transfer Port Numbers.
   a. Expand **Servers** > **Server Types** > **WebSphere application servers**, and click **MXServer** from the main window.
   b. Open the Web Container Settings and click **Web container transport chains**.
   c. Note the default port number as it appears with WCInboundDefault (9080).
9. Create the virtual host.
   a. Expand **Environment**.
   b. Click **Virtual Hosts**.
   c. Click **New**.
   d. In the General Properties section, type `maximo_host` in the Name box.
   e. Click **Apply**.
   f. Click **Save**.
   g. Click **OK**.
   h. From the Virtual Hosts window, click **maximo_host**.
   i. Click the **Host Aliases** link.
   j. Click **New**.
   k. Type `*` (asterisk) for host name and type the HTTP port number (by default `80`).
   l. Click **OK**.
   m. Click **New**.
   n. Type `*` (asterisk) for host name and type `9061` for the port number.
   o. Click **OK**.
   p. Click **New**.
   q. Type `*` (asterisk) for host name and type `9443` for the port number.
   r. Click **OK**.
   s. Click **New**.
   t. Type `*` (asterisk) for host name and type `9080` for the port number.
   u. Click **OK**.
   v. Click **New**.
   w. Type `*` (asterisk) for host name and type `9044` for the port number.
   x. Click **OK** and then click **Save**.
10. Enable automatic startup of the application server when the node agent is started.
   a. Expand **Servers** > **Server Types** > **WebSphere application servers**.
   b. Click **MXServer** in the main window.
   c. From the Server Infrastructure group, expand **Java and Process Management**.
   d. Click **Monitoring Policy**.
   e. Set Node restart state to **RUNNING** and click **OK**.

f. Click **Save** in the messages box.

   If you used the middleware installation program to install WebSphere Application Server Network Deployment v7, this step has already been performed by the middleware installation program.

Creating a Windows service for the node agent:

You can create a Windows service for starting the WebSphere Application Server Network Deployment node agent.

About this task

Although not required, you can optionally start the node agent as a Windows service.

If you used the middleware installation program to install WebSphere Application Server Network Deployment v7, this step has already been performed by the middleware installation program.

Procedure

1. Open a command prompt.
2. Change directory to `<WAS_HOME>\bin`.
3. Type the following command with no line breaks (case-sensitive).

   ```
   WASService
   -add NodeAgent
   -serverName nodeagent
   -profilePath "C:\IBM\WebSphere\AppServer\profiles\ctgAppSrv01"
   -wasHome "C:\IBM\WebSphere\AppServer"
   -logRoot "C:\IBM\WebSphere\AppServer\profiles\ctgAppSrv01\logs\nodeagent"
   -logFile "C:\IBM\WebSphere\AppServer\profiles\ctgAppSrv01\logs\nodeagent\
   startServer.log"
   -restart true
   ```
4. Close the Command Prompt.

Manually configuring JMS queues:

This procedure provides details on steps to configure JMS queues, which must be completed before using the product installation program.

About this task

During the installation process, the Maximo Asset Management installation program provides you with the option of automatically configuring Maximo Asset Management middleware. If you elect to have the Maximo Asset Management installation program automatically configure Maximo Asset Management middleware, it creates and configures JMS message queues for you. If you elect to manually configure Maximo Asset Management middleware for use with Maximo Asset Management, you must manually configure these message queues.

To configure the JMS queues, complete the following steps:

Procedure

1. Start the WebSphere Application Server Network Deployment application server.

2. Start Internet Explorer and open the WebSphere Application Server Network Deployment administrative console by typing the following URL:

   ```
   http://<server_name>:<port_number>/ibm/console
   ```

   For example, enter a URL like the following sample URL:

   ```
   http://localhost:9060/ibm/console
   ```
3. At the login screen, enter your user ID, then click **Log in**. This action opens the Welcome screen for the WebSphere Application Server Network Deployment administrative console.
4. Click **Service Integration** > **Buses** to open the Buses dialog. A bus is a group of interconnected servers and clusters that have been added as members of the bus.
5. Click **New** to open the **Create a new Service Integration Bus** panel where you can add a new service integration bus.
6. Enter `intjmsbus` as the name of the new bus in the Name field.
7. Clear the **Bus security** check box. If you leave this box checked, intjmsbus inherits the Global Security setting of the cell.
8. Click **Next**.
9. Click **Finish**.
10. Click **Save**. This step propagates the JMS bus setup to the cluster configuration.

Adding a server to the service integration bus:

A server must be defined for the service integration bus.

About this task

Complete the following steps to add a server to the service integration bus:

Procedure

1. From the WebSphere Application Server Network Deployment administrative console, click **Service Integration** > **Buses** to open the Buses dialog box.
2. Click **intjmsbus** to open the **Buses** > **intjmsbus** dialog box.
3. Under Topology, click **Bus members**.
4. In the **Buses** > **intjmsbus** > **Bus members** dialog box, click **Add** to open the Add a new bus member dialog box.
5. Select the **Server** option, and select the server name **ctgNode01:MXServer** to add to the bus, and then click **Next**.
6. Check that the **File store** radio button is selected, and then click **Next**.
7. From the Configure file store panel, click **Next**.
8. From the Tune application server for messaging performance panel, click **Next**.
9. Click **Finish**.
10. Click **Save**.
11. Select **intjmsbus**.
12. Change the value of the **Default messaging engine high message threshold** field to a minimum value of `500,000` messages, and then click **Apply**.

    If the number of messages awaiting processing exceeds the High Message Threshold you set, the application server limits the addition of new messages in the processing queues.

Depending on your message requirements, you can to enter a higher message threshold value. You can determine an optimal message threshold setting by monitoring the messaging in/out queues and the impact of the message threshold setting on system performance. You might, for example, lower the threshold value if a higher value is degrading system performance.

If you decide to change the High message threshold setting after the initial configuration, you must open the Additional Properties menu in the administrative console and change the threshold value for each child configuration.

13. Click **Save**.

Creating the service integration bus destination for the continuous inbound (CQINBD) queue:

You must create a service integration bus destination for the continuous inbound (CQINBD) queue.

About this task

To add a logical address for the continuous inbound bus destination queue (CQINBD) within the JMS bus, complete the following steps:

Procedure

1. From the WebSphere Application Server Network Deployment Administrative Console, click **Service Integration** > **Buses** to open the Buses dialog box.
2. Click **intjmsbus** to open the **Buses** > **intjmsbus** dialog box.
3. Click **Destinations** under Destination resources to open the **Buses** > **intjmsbus** > **Destinations** dialog box.

   A bus destination, for example CQINBD, is a virtual place within a service integration bus where applications can attach and exchange messages.
4. Click **New** to open the Create new destination dialog box.
5. Leave **Queue** checked as the destination type, and click **Next** to open the Create new queue dialog box.
6. Type `CQINBD` in the Identifier field and `Continuous Queue Inbound` in the Description field, then click **Next** to open the Create a new queue for point-to-point messaging dialog box.
7. Select the Bus Member pull-down and choose **Node=ctgNode01:Server=MXServer** as the bus member that will store and process messages for the CQINBD bus destination queue.
8. Click **Next** to open the Confirm queue creation dialog box.
9. Review your selections, then click **Finish** to complete the creation of the CQINBD bus destination queue.
10. Navigate the path **Buses** > **intjmsbus** > **Destinations**, then click **CQINBD** to open the configuration dialog box.
11. Click **None** as the Exception destination value.
12. Click **Apply**.
13. Click **Save**.

Creating the service integration bus destination for the sequential inbound (SQINBD) queue:

You must create the service integration bus destination for the sequential inbound (SQINBD) queue.

About this task

To add a logical address for the sequential inbound bus destination queue (SQINBD) within the service integration bus, complete the following steps:

Procedure

1. From the WebSphere Application Server Network Deployment Administrative Console, click **Service Integration** > **Buses** to open the Buses dialog box.
2. Click **intjmsbus** to open the **Buses** > **intjmsbus** dialog box.
3. Click **Destinations** under Destination resources to open the **Buses** > **intjmsbus** > **Destinations** dialog box. A bus destination is a virtual place within a service integration bus where applications can attach and exchange messages.
4. Click **New** to open the Create new destination dialog box.
5. Leave **Queue** checked as the destination type, and click **Next** to open the Create new queue dialog box.
6. Enter `SQINBD` in the Identifier field and `Sequential Queue Inbound` in the Description field, then click **Next** to open the Create a new queue for point-to-point messaging dialog box. Note that you must use this value and it must contain only uppercase letters.
7. Select the Bus Member pull-down and choose **Node=ctgNode01:Server=MXServer**
8. Click **Next** to open the Confirm queue creation dialog box.
9. Review your selections, then click **Finish** to complete the creation of the SQINBD bus destination queue.
10. Navigate the path **Buses** > **intjmsbus** > **Destinations**, then click **SQINBD** to open the configuration dialog box.
11. Click **None** as the Exception destination value.
12. Click **Apply**.
13. Click **Save**.

Creating the service integration bus destination for the sequential outbound (SQOUTBD) queue:

You must create the service integration bus destination for the sequential outbound (SQOUTBD) queue.

About this task

To add a logical address for the sequential outbound bus destination queue (SQOUTBD) within the service integration bus, complete the following steps:

Procedure

1. From the WebSphere Application Server Network Deployment administrative console, click **Service Integration** > **Buses** to open the Buses dialog box.
2. Click **intjmsbus** to open the **Buses** > **intjmsbus** dialog box.
3. Click **Destinations** under Destination resources to open the **Buses** > **intjmsbus** > **Destinations** dialog box. A bus destination, for example

SQOUTBD, is a virtual place within a service integration bus where applications can attach and exchange messages.

4. Click **New** to open the Create new destination dialog box.
5. Leave **Queue** checked as the destination type, and click **Next** to open the Create new queue dialog box.
6. Enter `SQOUTBD` in the Identifier field and `Sequential Queue Outbound` in the Description field, then click **Next** to open the Create a new queue for point-to-point messaging dialog box. You must use this value and it must contain only uppercase letters.
7. Select the Bus Member menu and choose **Node=ctgNode01:Server=MXServer** as the bus member that stores and processes messages for the SQOUTBD bus destination queue.
8. Click **Next** to open the Confirm queue creation dialog box.
9. Review your selections, then click **Finish** to complete the creation of the queue.
10. Navigate the path **Buses** > **intjmsbus** > **Destinations**, then click **SQOUTBD** to open the configuration dialog box where you must make the following changes:
11. Click **None** as the Exception destination value.
12. Click **Apply**.
13. Click **Save**.

Creating the JMS connection factory:

Add a connection factory for creating connections to the associated JMS provider of point-to-point messaging queues.

About this task

To create the JMS connection factory, complete the following steps:

Procedure

1. From the WebSphere Application Server Network Deployment administrative console, click **Resources** > **JMS** > **Connection factories**.
2. From the **Scope** drop-down list, select **Cell=ctgCell01**.
3. Click **New**.
4. Verify that the Default Messaging Provider is selected and click **OK**.
5. Enter the following information:

   Name Enter `intjmsconfact`.

   JNDI name
   Enter `jms/maximo/int/cf/intcf`.

   Bus name
   Select **intjmsbus**.
6. Click **Apply**.
7. Click **Save**.

Creating the continuous inbound (CQIN) JMS queue:

You must create a JMS queue (CQIN) as the destination for continuous inbound point-to-point messages.

About this task

To create the CQIN JMS queue, complete the following steps:

Procedure

1. From the WebSphere Application Server Network Deployment administrative console, click **Resources** > **JMS** > **Queues**.
2. From the Scope drop-down list, select **Cell=ctgCell01**.
3. Click **New**.
4. Verify that the Default Messaging Provider is selected and click **OK**.
5. Enter the following information, and click **OK**.

   Name Enter `CQIN`.

   This value must contain only uppercase letters.

   JNDI name
   Enter `jms/maximo/int/queues/cqin`

   Bus name
   Select **intjmsbus**.

   Queue name
   Select **CQINBD**.
6. Click **OK**.
7. Click **Save**.

Creating the sequential inbound (SQIN) JMS queue:

You must create a JMS queue (SQIN) as the destination for sequential inbound point-to-point messages.

About this task

To create the SQIN JMS queue, complete the following steps:

Procedure

1. From the WebSphere Application Server Network Deployment administrative console, click **Resources** > **JMS** > **Queues**.
2. From the Scope drop-down list, select **Cell=ctgCell01**.
3. Click **New**.
4. Verify that the Default Messaging Provider is selected and click **OK**.
5. Enter the following information, and click **OK**.

   Name Enter `SQIN`.

   This value must contain only uppercase letters.

   JNDI name
   Enter `jms/maximo/int/queues/sqin`

   Bus name
   Select **intjmsbus**.

   Queue name
   Select **SQINBD**.
6. Click **OK**.
7. Click **Save**.

Creating the sequential outbound (SQOUT) JMS queue:

You must create a JMS queue (SQOUT) as the destination for sequential outbound point-to-point messages.

About this task

To create the SQOUT JMS queue, complete the following steps:

Procedure

1. From the WebSphere Application Server Network Deployment administrative console, click **Resources** > **JMS** > **Queues**.
2. From the Scope drop-down list, select **Cell=ctgCell01**.
3. Click **New**.
4. Verify that the Default Messaging Provider is selected and click **OK**.
5. Enter the following information, and click **OK**.

   Name Enter `SQOUT`.

   This value must contain only uppercase letters.

   JNDI name
   Enter `jms/maximo/int/queues/sqout`

   Bus name
   Select **intjmsbus**.

   Queue name
   Select **SQOUTBD**.
6. Click **OK**.
7. Click **Save**.

Creating JMS activation specification for the continuous inbound queue (CQIN):

You must activate the continuous inbound queue (CQIN) before it can receive messages.

About this task

Complete the following steps to activate the CQIN queue:

Procedure

1. From the WebSphere Application Server Network Deployment administrative console, click **Resources** > **JMS** > **Activation Specifications**.
2. From the Scope drop-down list, select **Cell=ctgCell01**.
3. Click **New**.
4. Select **Default messaging provider** and then click **OK**.
5. Enter the following information, and then click **OK**.

   Name `intjmsact`

   This value is case-sensitive. This value must be lowercase.

   JNDI name
   `intjmsact`

   Destination type
   `Queue`

Destination JNDI name
`jms/maximo/int/queues/cqin`

Bus name
intjmsbus

Maximum concurrent MDB invocations per endpoint
`10`

6. Click **OK**, and then click **Save**.

Error queues:

You must create an error queue that receives redirected messages from the continuous queue (CQIN).

When the messages go in error, the error queue receives redirected messages from the continuous queue (CQIN).

Creating the service integration bus destination for the inbound error queue (CQINERRBD) queue:

You must add a logical address for the inbound error queue (CQINERRBD) queue within the JMS bus.

About this task

Perform the following steps:

Procedure

1. From the WebSphere Application Server Network Deployment administrative console, click **Service Integration** > **Buses** to open the Buses dialog box.
2. Click **intjmsbus** to open the **Buses** > **intjmsbus** dialog box.
3. Click **Destinations** under Destination resources to open the **Buses** > **intjmsbus** > **Destinations** dialog box. A bus destination is a virtual place within a service integration bus where applications can attach and exchange messages.
4. Click **New** to open the Create new destination dialog box.
5. Leave **Queue** checked as the destination type, and click **Next** to open the Create new queue dialog box.
6. Enter `CQINERRBD` in the Identifier field and `Error Queue Inbound` in the Description field, then click **Next** to open the Create a new queue for point-to-point messaging dialog box. You must use this value and it must contain only uppercase letters.
7. From the Bus Member menu, select **Node=ctgNode01:Server=MXServer**
8. Click **Next** to open the Confirm queue creation dialog box.
9. Review your selections, then click **Finish** to create the CQINERRBD bus destination queue.
10. Select **Buses** > **intjmsbus** > **Destinations**, then click **CQINERRBD** to open the configuration dialog box where you must make the following changes:
    a. Select the **Specify** option and enter `CQINERRBD` as the exception destination value.
    b. Change the Maximum failed deliveries value to `5`.

This option is the maximum number of times you want the system to process a failed messaging attempt before forwarding the message to the exception destination.

11. Click **Apply**.
12. Click **Save**.
13. From the WebSphere Application Server Network Deployment administrative console, click **Service Integration** > **Buses** to open the Buses dialog box.
14. Click **intjmsbus** to open the **Buses** > **intjmsbus** dialog box.
15. Click **Destinations** under Destination resources to open the **Buses** > **intjmsbus** > **Destinations** dialog box.
16. Select **CQINBD**.
17. Specify `CQINERRBD` as the exception destination. Set the Maximum failed deliveries value to `5`.
18. Click **OK**.
19. Click **Save**.

Creating the error (CQINERR) JMS queue:

After creating the Error Queue Bus Destination, you create the Error queue.

About this task

To create the Error queue, complete the following steps.

Procedure

1. From the WebSphere Application Server Network Deployment administrative console, click **Resources** > **JMS** > **Queues**.
2. From the Scope drop-down list, select **Cell=ctgCell01**.
3. Click **New**.
4. Verify that the Default Messaging Provider is selected and click **OK**.
5. Enter the following information, and click **OK**.

   Name Enter `CQINERR`.

   This value must contain only uppercase letters.

   JNDI name
   Enter `jms/maximo/int/queues/cqinerr`

   Bus name
   Select **intjmsbus**.

   Queue name
   Select **CQINERRBD**.
6. Click **OK**.
7. Click **Save**.

Creating JMS activation specification for the inbound error queue (CQINERR):

You must activate the continuous inbound queue (CQINERR) before it can receive messages.

About this task

Complete the following steps to activate the CQINERR queue:

Procedure

1. From the WebSphere Application Server Network Deployment administrative console, click **Resources** > **JMS** > **Activation Specifications**.
2. From the Scope menu, select **Cell=ctgCell01**, and then click **Apply**.
3. Click **New** to complete the General Properties section for the new JMS activation specification.
4. Click **OK**.
5. Enter the following information, and click **OK**.

   Name Enter `intjmsacterr`.

   This value must only contain lowercase letters.

   JNDI name
   Enter `intjmsacterr`.

   This value must be the same as the one used for the **Name** field.

   Destination type
   Enter `Queue`.

   Destination JNDI name
   `jms/maximo/int/queues/cqinerr`

   Bus name
   intjmsbus

   Maximum concurrent MDB invocations per endpoint
   `10`
6. Click **OK**.
7. Click **Save**.
8. Ensure that you stop all IBM-related processes and daemons.
9. You must now restart these processes for the update to take effect.
10. Start the bus member for the ctgNode MXServer intjmsbus if it is not started. If you cannot start ctgNode MXServer intjmsbus, restart MXServer under **Servers** > **Application servers**.

Manually creating a data source for the persistent store:

If you chose to manually configure WebSphere Application Server Network Deployment, you must create a data source in order to store JMS messages in a DB2 database.

About this task

You have the option of having WebSphere Application Server Network Deployment use a DB2 database to store JMS messages. For more information about WebSphere Application Server Network Deployment message storage, including the usage of products other than DB2, see http://publib.boulder.ibm.com/infocenter/wasinfo/v7r0/index.jsp?topic=/com.ibm.websphere.nd.multiplatform.doc/info/ae/ae/tjm0045_.html.

To create a data source for the persistent store, complete the following steps:

Procedure

1. Create a system user and password on the server hosting the database server. For example, a user named `mxsibusr` with a password of `mxsibusr`.

2. Create and configure the database.
   a. Open DB2 Control Center.
   b. Browse to the Databases folder listed under your system.
   c. Right-click the Databases folder and select **Create Database** > **Standard**.
   d. Create a database named `maxsibdb` using default settings.
   e. After the database has been created, expand the maxsibdb database and select **User and Group objects**.
   f. Right-click **DB Users** and select **Add**.
   g. Select **mxsibusr** from the User menu.
   h. Grant all authorities to the mxsibusr except Security administrator authority.
   i. Click **Apply**.
   j. Verify that you can connect to the database using the mxsibusr user by right-clicking **maxsibdb** and selecting **Connect**.
3. Configure J2C authentication data and JDBC provider in WebSphere Application Server Network Deployment.
   a. Open and login to the WebSphere Application Server Network Deployment administrative console.
   b. Browse to **Security** > **Global Security**.
   c. Under the Authentication header, click **Java Authentication and Authorization Service** > **J2C authentication data**.
   d. Click **New**.
   e. Complete the following fields in the User identity form.

      Alias `maxJaasAlias`

      User ID
      `mxsibusr`

      Password
      Password you created for mxsibusr.

      Description
      SIB database user alias.
   f. Click **Apply**, and then click **Save**.
   g. From the WebSphere Application Server administrative console, browse to **Resources** > **JDBC** > **JDBC Providers**.
   h. Under **Scope**, click **Show scope selection drop-down list with the all scopes option**, select **Cell=ctgCell01**, and then, under **Preferences**, click **Apply**.
   i. Click **New**.
   j. Specify the following values, and then click **Apply**:

      Database type
      DB2

      Provider type
      DB2 Universal JDBC Driver Provider

      Implementation type
      XA data source

      Name **maxJdbcProvider**
   k. Click **Next**.

l. Complete the WebSphere Application Server variable ${DB2UNIVERSAL_JDBC_DRIVER_PATH} field with a value of `<WAS_HOME>ctgMX\lib`. For example, `C:\Program Files\IBM\WebSphere\AppServer\ctgMX\lib`.

m. Click **Next**.

n. Click **Finish**.

o. Click **Save**.

4. Open a command prompt and copy `<DB2_HOME>/java/db2jcc.jar` and `<DB2_HOME>/java/db2jcc_license_cu.jar` to the `<WAS_HOME>\ctgMX\lib` directory. Go back to **Resources** > **JDBC** > **JDBC Providers** > **maxJdbcProvider**, and correct the class path if required for both `db2jcc.jar` and `db2jcc_license_cu.jar`. Ensure that each jar file has the full path from ${DB2UNIVERSAL_JDBC_DRIVER_PATH}
5. Configure WebSphere Application Server:
   a. From the WebSphere Application Server Network Deployment administrative console, browse to **Resources** > **JDBC** > **Data sources**.

   b. Under **Scope**, click **Show scope selection drop-down list with the all scopes option**, select **Cell=ctgCell01**, and then, under **Preferences**, click **Apply**.

   c. Click **New**.

   d. Specify the following values:

      Data source name
         intjmsds

      JNDI name
         jdbc/intjmsds

   e. From the Component-managed authentication alias and XA recovery authentication alias menu, select **maxJaasAlias**

   f. Click **Next**.

   g. Choose **Select an existing JDBC provider**, and then select **maxJdbcProvider** from the menu.

   h. Click **Next**.

   i. Specify the following values:

      Database name
         `maxsibdb`

      Driver type
         `4`

      Server name
         Specify the DB2 server host name.

      Port number
         Specify the DB2 port number. For example, `50005`.

   j. Ensure the **Use this data source in container managed persistence (CMP)** option is selected, and then click **Next**.

   k. Click **Finish**.

   l. Click **Save**.
6. Verify the data source by selecting **intjmsds**, and then clicking **Test Connection**.

Installing the product and manually configuring middleware

You can deploy Maximo Asset Management with configured middleware before the installation begins. You use this procedure if your organization has specific policies and procedures that govern how you create databases, database instances, and users within your organization.

Before you begin

Ensure that you meet prerequisite conditions.

- The database server, the directory server, and application server services must be started and active.
- The `/tmp` and `/var/tmp` directories must be present on the system. The installation program depends on these directories for information during deployments on IBM WebSphere Application Server Network Deployment.
- On the administrative workstation, temporarily shut down any noncritical processes that can have a negative effect on the installation, such as antivirus software.
- Ensure that the Windows DEP setting does not prevent the launchpad from running: Select **Start** > **Settings** > **Control Panel** > **System** > **Advanced** > **Performance** > **Settings** > **Data Execution Prevention**. Select **Turn on DEP for essential Windows programs and services only** and click **Apply**. You might be asked to reboot the server.
- For Linux and UNIX systems with middleware installed, the command **`hostname -f`** must return a fully qualified host name. If necessary, consult the documentation for your operating system. Alternatively, you can provide the IP address for the system.
- Enable a remote execution and access service on every system that has middleware installed. Each remote system must support a remote access protocol. Each system must accept remote logins from a user name and password that were configured on the target server. Remote access protocols include SSH and Windows SMB. If the remote system is a Windows server, you must configure remote execution and access to use SMB.

About this task

The instructions are for a multiple server installation that uses default values.

Procedure

1. Log in on the administrative system.
2. Start the product installation program from the launchpad.
   a. Start the launchpad. Browse to the root directory of the downloaded installation image, and run the following command:

      Windows

      ```
      launchpad.exe
      ```

   b. In the launchpad navigation pane, click **Install**.
   c. Click **Install Maximo Asset Management 7.5**.

   If the launchpad does not start the installation, you can start the product installation program directly. On the downloaded installation image, browse to `\Install\mam\`, and run one of the following commands:

   Windows

   - `install.bat`

- `install_win64.bat`

3. Select a language for the installation and click **OK**.
4. On the Choose Installation Folder panel, specify the path to the location where you want to install Maximo Asset Management.

   You can specify a description for the installation. A description is useful for differentiating between multiple installations that are hosted on the same administrative workstation.
5. Review the information that is on the Verify Installation Location panel. The panel shows any previous installation information that was found based on the installation directory that you specified on the previous panel. After you advance past this panel, you cannot go back and change the installation directory for this installation.

   If a more recent version of the installation program is found in the specified target directory, you are notified. The notification means that you are using an older version of the installation program. The version found on the administrative workstation is newer and can contain important features and enhancements. To use the newer version of the installation program, select the option on the notification panel and click **Next**. This action exits the current installation process and restarts the installation process with the newer installation program. If you do not select the option, you continue the installation with the older version of the installation program.
6. On the Package Summary panel, review the package deployment information. This panel lists version information for both new and existing packages on the system. Target package version information indicates the package version being currently deployed.
7. On the Choose Deployment panel, specify **Simple** or **Custom** as the deployment type.
8. On the Import Middleware Configuration Information panel, you select **Import middleware configuration information** to have the product installation program reuse the middleware installation program values. These values are used as default values for the same fields in the product installation program.

   The **Workspace location** field refers to the location of the topology file that contains the values that were specified for the middleware installation program. The file is located in the workspace that was defined during the middleware installation task. For example, `C:\ibm\tivoli\mwi\workspace` for Windows or `/root/ibm/tivoli/mwi/workspace` for UNIX.

   If you selected the simple deployment, the middleware default information is not used.
9. On the Database Type panel, specify the software to use for the Maximo database.
10. On the Database panel, specify configuration information for your database software.

    For things such as the database user ID, the database name, the database instance for Maximo Asset Management, and the schema name, if the values do not exist when you specify them, they are created. Database users and database instance names cannot contain spaces.

    After you specify configuration information for your database software, the installation program validates the information with the database server.
11. On the Automate Database Configuration panel, select **The database has already been created and configured** and click **Next**.

This step assumes that you created a database instance, a database, table spaces, a user, and schema for use with Maximo Asset Management. See "Manually configuring the database" on page 55. If you have not manually configured the database before selecting **The database has already been created and configured** you are prompted to complete them before you restart the installation program.

12. On the Database Tablespace panel, specify information about the table space of the database.

    When you click **Next**, the product installation program connects to the database server and validates the information that you specified.
13. When the database validation is complete, on the Application Server Type panel, specify the application server type for the product deployment.

    You have the option of configuring WebSphere Application Server Network Deployment automatically through the product installation program.
14. On the WebSphere Connectivity panel, specify host information for the WebSphere Application Server Network Deployment.
15. On the WebSphere Remote Access Authorization panel, specify authorization information for WebSphere Application Server Network Deployment configuration.
16. On the WebSphere Application Server Network Deployment Configuration panel, specify configuration information for WebSphere Application Server Network Deployment.

    The web server port should match an existing HTTP server port value that you configured when you set up WebSphere Application Server Network Deployment. If you specify a different value for the web server port, you must restart WebSphere Application Server Network Deployment at the conclusion of the installation. Restarting the server activates the new port and makes it available for incoming requests.

    The application server name that you specify is created if it does not exist.
17. On the Security panel, specify the method to use for authenticating and authorizing users.
18. On the Specify Maximo Users panel, enter Maximo database user information.

    Maximo administration user
    The product administrator user ID that is used for initial configuration and adding users.

    Maximo system registration user
    The user ID that is used for the self-registration of users.

    Maximo system integration user
    The user ID that is used with enterprise adapters.

    Custom user ID and password values are stored in the Maximo database. The default user IDs of maxadmin, maxreg, and maxintadm are also created as users in the Maximo database. Creation of the default user IDs is done for internal processing purposes. If you use Maximo database security for authentication and authorization, the default user IDs can be used to log in to the application. If you regard this condition as a security risk, you can modify the passwords for the default user IDs. You modify passwords for the user IDs in the Users application.
19. On the Security panel, specify the names of the user and group base entries and specify how Maximo Asset Management users are created.

User base entry

If you do not plan to use the default LDAP schema that is provided with Maximo Asset Management, specify the user base entry that you want to use.

Group base entry

If you do not plan to use the default LDAP schema, specify the group base entry that you want to use.

You can specify that the installation program creates the required users. Otherwise, you must create users manually before you continue.

If you are not using the default LDAP schema that is provided, you must create it yourself before you advance beyond this panel. The values that are specified for the **User base entry** and **Group base entry** fields are used to configure the VMMSYNC cron task. To create your own LDAP schema and create users manually, you can modify the default add-on LDIF data and import it into your LDAP repository

20. On the Integration Adapter JMS Configuration panel, specify Java Message Service configuration information. A JMS server requires a DB2 data repository to be configured to maintain messages. If you are using another database type, you cannot configure message persistence. If you specify that JMS messages are not to be persisted, you can configure the JMS implementation manually later.

    Specify the name of the database to be used by JMS. For DB2, you can specify whether to persist JMS messages within DB2.

    Select **Do not persist JMS messages** if you are deploying Maximo Asset Management with Oracle or Microsoft SQL Server. When you click **Next**, the installation wizard skips to the SMTP Configuration panel.
21. In the WebSphere Application Server Network Deployment keystore file panel, browse to where you copied the trust.p12 keystore, and then click **Next**.
22. On the SMTP Configuration panel, specify the SMTP configuration information that is used by workflows to communicate with workflow participants.

    The administrator e-mail address is the e-mail address that is used to send messages. If you leave the fields blank, you must configure the SMTP parameters through the product interface as a post-installation task.
23. On the Base Language Selection panel, specify the base language for the installation.
24. On the Additional Language Selection panel, you can optionally specify one or more additional languages that the installation is to support.
25. On the Run Configuration Step panel, specify how to perform the configuration step of the installation. If you do not select an option, the configuration step proceeds when you click **Next**. You can optionally create a maxdemo database from the Run Configuration Step panel.

    Copy files now, but perform the installation configuration step later

    Select this option to copy files from the installation source to the administrative workstation. You must perform the configuration step at a later time to complete the deployment.

    Select this option to create a maxdemo database during the installation of Maximo Asset Management and populate the database with sample data.

    Important: Do not install another product before completing the configuration step of the original installation. Installing another product before running the configuration step for this installation overwrites the taskstore, which prevents the original installation from ever being deployed.

The configuration values that you specify are stored in the *install_home*\maximo\applications\maximo\properties\maximo.properties and *install_home*\etc\install.properties files. You run the configuration steps outside of the product installation program by using the taskrunner utility, in the *install_home*\scripts directory. Run the taskrunner utility from the command line.

```
install_home\scripts\taskrunner [CONTINUE <STOPONERROR|NOSTOPONERROR>]
```

The taskrunner uses the configuration values that are stored in the maximo.properties and install.properties files to configure Maximo Asset Management.

If you run taskrunner with the **NOSTOPONERROR** parameter, the taskrunner continues despite errors. If you run taskrunner with the **STOPONERROR** parameter, the taskrunner stops when it encounters an error. If you used **STOPONERROR**, you can rectify the conditions that caused the error. You can then resume the installation at the point where the last successfully completed task was recorded in the previous attempt by starting taskrunner with the **CONTINUE** parameter.

Deploy application files manually later
Select this option to manually deploy application files to the application server.

Defer the update of the Maximo database
Select this option if you want to manually run the database update task for the product deployment. This option can be used when there is a fix pack available that addresses known issues with the updatedb script. In this scenario, you choose the **Defer the update of the Maximo database** option, apply the fix pack, and then run the **updatedb -v1** command manually.

26. On the Choose Shortcut Folder panel, specify where you want Maximo Asset Management icons created.

    If you select **In the Start Menu** and use Internet Explorer, add the Maximo Asset Management URL to the trusted sites web content zone. Disable the option that requires server verification for all sites in the zone.

    Do not select **In the Quick Launch Bar**. The selection does not create a shortcut in the Quick Launch bar.

27. On the Input Summary panel, review the information that you have provided for the product installation program.

    If necessary, use **Previous** to return to previous panels to change values.

28. On the Pre-Installation Summary panel, review the installation information, then click **Install**.

    The installation process begins. You can monitor the progress of the installation by viewing the messages that are shown.

29. On the Installation Completed panel, review any information presented, then click **Done**.

What to do next

Complete the post installation tasks that are required for installing with manual middleware configuration.

If you selected the **Deploy application files manually later** option, you must now deploy the `maximo.ear` and `maximoiehs.ear` files.

“Deploying EAR files” on page 154
This section contains information about deploying Maximo Asset Management EAR files manually into WebSphere Application Server Network Deployment.

Creating a maxdemo database during installation

You can create a maxdemo database during a Maximo Asset Management installation and populate the database with sample data.

Procedure

1. On the Run Configuration Step panel of the installation wizard, select **Copy files now, but perform the installation configuration later**.
2. When the installation finishes, exit the installation wizard.
3. Rename the `C:\IBM\SMP\Maximo\tools\maximo\en\maximo.`*`dbtype`* file.
4. Copy the `C:\IBM\SMP\Maximo\tools\maximo\en\maxdemo.`*`dbtype`* file to `C:\IBM\SMP\Maximo\tools\maximo\en\maximo.`*`dbtype`*, where `en` is the language folder and the *dbtype* is `ora`, `sqs`, or `db2`.
5. Open a command window and browse to `C:\IBM\SMP\scripts`.
6. Run the following command: `taskrunner.bat CONTINUE STOPONERROR`
7. When the taskrunner process is complete, change the file names back to their original names. Do not restart the computer before you run the taskrunner command. The taskrunner utility does not create a persistent store of information and data can be lost.

Language deployment after database update deferral

Selecting the option to defer the update of the Maximo database when installing the product, affects how you deploy languages.

During installation, you have the option to defer the database update task. This option prevents writing data to the database during the installation. The installation program is limited to copying files to the administrative system and registering product process solution packages. You add languages by completing the installation, manually updating the database, and then updating languages manually.

“Manually deploying languages after database update deferral” on page 38
Languages must be deployed manually if you defer database updates by the installation program.

Manually deploying languages after database update deferral

Languages must be deployed manually if you defer database updates by the installation program.

Before you begin

You must have run updatedb command before manually configuring languages for PSI packages.

About this task

To manually configure languages for PSI packages, complete the following steps:

Procedure

Update language support for the Maximo core components.
Files for the language selections you made during the installation are extracted to the C:\IBM\SMP\Maximo\Tools\Maximo\locale\xliff\ directory on the system.

1. To update a language as the base language to use for the product, run the following command:

   ```
   install_home\maximo\tools\maximo\TDToolkit.bat
   -IMPORT
   -SLEN
   -TLlocale
   -maxmessfix
   ```

2. To add one or more languages as additional languages for use with the product, run the following command for each language you want to add:

   ```
   install_home\maximo\tools\maximo\TDToolkit.bat
   -ADDLANGlocale
   -maxmessfix
   ```

Chapter 5. Silent installation

Maximo Asset Management provides the option of installing silently.

The Maximo Asset Management silent installation option allows you to interface with the Maximo Asset Management installation program using a command prompt (not the Maximo Asset Management launchpad), and a response file.

Installing Maximo Asset Management silently

Maximo Asset Management can be installed silently by using an installation response file.

Before you begin

You must complete a successful Maximo Asset Management installation to produce a response file that can be used for a silent installation. Alternatively, you can use one of the sample response files that are provided on the product media and modify it according to your needs.

You must verify that all response file paths are formatted correctly. If a path such as `USER_INSTALL_DIR=K:/IBM/max_dev` is contained in a response file that is used with a Windows administrative system, an error occurs. The Windows equivalent in this example must be formatted for a Windows system: `USER_INSTALL_DIR=K:\\IBM\\max_dev`

Note: You can use a silent installation response file to populate Maximo Asset Management installation program fields during an attended installation. Remove the `INSTALLER_UI=silent` property from the response file before you use it with the Maximo Asset Management installation program. The installation program uses default values by reading from the response file. The Maximo Asset Management installation program uses the response file automatically when it is named `installer.properties` or `install.properties` and it is in the same directory. You do not have to specify the response file name when you start the Maximo Asset Management installation program.

Note: This response file can also be used with the Maximo Asset Management uninstallation program to uninstall Maximo Asset Management silently.

About this task

To install Maximo Asset Management silently, complete the following steps:

Procedure

1. Make configuration choices by using the Maximo Asset Management installation program, and record those choices in a response file:
   a. Start the Maximo Asset Management installation program from the product image. Use the following command for 32–bit systems:

      ```
      install.exe -r <response file path and name>
      ```

      For 64–bit systems, use the following command:

      ```
      install_win64.exe -r <response file path and name>
      ```

The Maximo Asset Management installation program executable files are in the Maximo Asset Management directory of the Maximo Asset Management 7.5 product image.

Response files must have a file extension of .properties, for example, `response.properties`.

You must include the full path when you specify the response file.

b. Proceed through the Maximo Asset Management installation program, making configuration choices.

c. Exit the Maximo Asset Management installation program after Maximo Asset Management is successfully installed.

There are several sample response files provided on the IBM Maximo Asset Management 7.5 product image.

Table 5. Maximo Asset Management installation program sample silent response files

File	Description
`simple_response.properties`	This file contains a sample response file that would be used to install a simple deployment of Maximo Asset Management.
`custom_response_win.properties`	This file contains a sample response file that would be used to install a custom deployment of Maximo Asset Management on Windows.

The files are in the `Maximo Asset Management\samples` directory of the product image.

If the response file is created by recording an actual installation, you must add an entry for LICENSE_ACCEPTED=true. If you are using a sample response file, you must change the entry from `false` to `true`. If a silent installation is started and this entry is not included in the response file then the installation ends immediately. No messages or log file are created.

If you plan to deploy Maximo Asset Management using middleware hosted on both Windows and UNIX operating systems, your response file contains both Windows and UNIX values. These values include directory paths and executable file names. In some cases, the response file is not generated because the user who starts the installation program does not have write access to the target directory. In this scenario, the installation program does not report an error. The response file is not written to the target directory and the log file is not produced in the `ibm\smp\logs` directory. To resolve this issue, ensure that the user who starts the installation program has write access to the target directory before they run the installation program.

2. Open the response file in a text editor and change the INSTALLER_UI property to INSTALLER_UI=silent. Passwords are stored in clear text format. You must edit the CONFIRM_PASSWORD fields contained in the response file to match its corresponding password value used for each task. For example, ensure that CONFIRM_PASSWORD matches RXA_PASSWORD in the following example:

```
#Middleware Server Information
#----------------------------
MIDDLEWARE_SERVER=myserver.mydomain.com
RXA_USER_ID=root
RXA_PASSWORD=mypassword
CONFIRM_PASSWORD=mypassword
```

3. Copy the response file to the target system.

4. Start the Maximo Asset Management installation program silently and identify the response file to be used.

```
install.exe -f <response file path and name>
```

You must include the full path when you specify the response file and it must be on the C:\ drive of your system.

Results

The installation proceeds silently with the values that you provided in the response file.

Response files that include fields for Oracle configuration must be edited to remove extraneous backslashes. A response file that includes Oracle as a deployment option is generated with fields like the following excerpt:

```
DB_INSTALL_DIR=C\:/oracle/product/10.2.0/db_1
INSTANCE_LOCATION=C\:/oracle/product/10.2.0/db_1/dbs
WAS_HOME_DIR=C\:/Program Files/IBM/WebSphere/AppServerUSER_INSTALL_DIR=C\:/IBM/
USER_SHORTCUTS=C\:/Documents and Settings/All Users/Start Menu/Programs
 /process automation engine
MAXIMO_INSTALL_DIR=C\:/IBM/maximo
```

You must remove the backslash that is directly after the drive letter, so that your response file looks like following excerpt:

```
DB_INSTALL_DIR=C:/oracle/product/10.2.0/db_1
INSTANCE_LOCATION=C:/oracle/product/10.2.0/db_1/dbs
WAS_HOME_DIR=C:/Program Files/IBM/WebSphere/AppServerUSER_INSTALL_DIR=C:/IBM/
USER_SHORTCUTS=C:/Documents and Settings/All Users/Start Menu/Programs
 /process automation engine
MAXIMO_INSTALL_DIR=C:/IBM/maximo
```

If you attempt to install Maximo Asset Management silently and the installation UI is shown, check inside the response file to ensure that it contains this line:

```
INSTALLER_UI=silent
```

Silent installation properties

Silent installation properties are recorded in an installation response file. Silent installation response files are generated when the installation program is started with the parameters described in the silent installation procedure. Alternatively, a silent installation response file can be created and populated manually.

Common silent installation properties

The following properties are common to all deployments.

Table 6. Common silent installation response file properties

Category	Property	Definition
File header	INSTALLER_UI=SILENT	This property must be set so the file can be used with the product installation program.
Package deployment set	INSTALL_SOME_PACKAGES=0	If only a subset of packages can be installed, set this value to **1**. This setting allows the product installation program to continue.
License Agreement	LICENSE_ACCEPTED=TRUE	Set this value to **true** to accept the license agreement or **false** to reject it.

Table 6. Common silent installation response file properties (continued)

Category	**Property**	**Definition**
Installation folder	USER_INSTALL_DIR=*installation path*	Set an installation path. For example, for Windows, `C:\\IBM\\SMP`.
Installation description	INSTALLATION_DESCRIPTION	Description of the installation location.
Deployment type	SIMPLE=0	Installation is set to a type of SIMPLE. Set to **0** to disable. Set to **1** to enable. If SIMPLE is enabled, ADVANCED must be disabled.
	ADVANCED=1	Installation is set to a type of ADVANCED, which is a Custom installation. Set to **0** to disable. Set to **1** to enable. If ADVANCED is enabled, SIMPLE must be disabled.
Middleware Server Information (only used for Simple installations)	MIDDLEWARE_SERVER=*host name*	Set the host name of the system that is hosting all middleware.
	RXA_USER_ID=*user name*	Set the user ID for accessing the system that is hosting all middleware.
	RXA_PASSWORD=*password*	Set a password for the user ID for accessing the system that is hosting all middleware.
Import Middleware installation program information	MWI_IMPORT_DATA=0	Set this parameter to import configuration data from the middleware installation program. Set to **0** to disable. Set to **1** to enable.
	MWI_HOSTNAME=*host name*	Set the host name of the system that is hosting the middleware installation program workspace.
	MWI_USER_ID=*user name*	Set a user ID used to access the system that is hosting the middleware installation program workspace. For example, **root**.
	MWI_PASSWORD=*passsword*	Set a password for the user ID used to access the system that is hosting the middleware installation program workspace.
	MWI_LOCATION=*path*	Set a path for the location of the middleware installation program workspace. For example, for Windows, `C:\\ibm\\tivoli\\mwi\\workspace`.

Table 6. Common silent installation response file properties (continued)

Category	Property	Definition
SMTP Configuration	SMTP_SERVER=*host name*	Set the name of the system that is hosting the SMTP server responsible for distributing administration messages to the Maximo Asset Management administrator.
	ADMIN_EMAIL=*email address*	Set the email address for the Maximo Asset Management administrator.
Run Configuration Step	RUN_CONFIG_NO=0	Set the behavior of the run configuration step. Set to **0** to disable (run the configuration step at installation time). Set to **1** to enable (defer the configuration step).
	DEPLOY_EAR_NO=0	Set the behavior of the EAR deployment step. Set to **0** to disable (deploy the EAR at installation time). Set to **1** to enable (defer deployment of the EAR).
	DEFER_DB_UPDATE=0	Set the behavior of the database update step. Set to **0** to disable (run updateDB at installation time). Set to **1** to enable (defer updateDB).
Shortcut Folder	USER_SHORTCUTS=*path*	Set a path for shortcuts. For example, for Windows, `C:\\Documents and Settings\\Administrator\\Desktop\\process automation engine`.
Installer version	LAUNCH_NEW_INSTALLER=TRUE	If a more recent version of the installation program was found in the target installation directory specified. This circumstance indicates that you are using an older version of the installation program. In order to use the newer version of the installation program, set this value to **TRUE**. If you set this value to **FALSE**, the older version of the installation program is used to perform the installation.

Users silent installation properties

The following properties are for users created by or identified to the installation program.

Table 7. Users silent installation properties

Category	Property	Definition
User Information	MAXADMIN_USER_NAME=*user name*	Set a user name for the Maximo administrator. For example, **maxadmin**.
	MAXADMIN_PASSWORD=*password*	Set a password for the Maximo administrator. For example, **maxadmin**.
	MAXREG_USER_NAME=*user name*	Set a user name for the self registration user. This user is responsible for the process by which users can create their own accounts. For example, **maxreg**.
	MAXREG_PASSWORD=*password*	Set a password for the self registration user. For example, **maxreg**.
	MXINTADM_USER_NAME=*user name*	Set a user name for the internal user. For example, **mxintadm**.
	MXINTADM_PASSWORD=*password*	Set a password for the internal user. For example, **mxintadm**.

Common database silent installation properties

The following properties contain common information about the database used for the deployment.

Table 8. Common database silent installation response file properties

Category	Property	Definition
	DB_TYPE_ORACLE=0	Set the database type to Oracle. Set to **0** to disable. Set to **1** to enable. Only one Database Type can be enabled.
Database	DB_HOST_NAME=*host name*	Set the host name of the database server.
	DB_PORT=*port*	Set the database port. For example, **50005**.
	DB_INSTANCE=*instance*	Set a name for the database instance to use with the product. For example, **ctginst1**. Oracle
	DB_USER=*user name*	Set the name of the user ID to access the database. For example, **maximo**.
	DB_PASSWORD=*password*	Set a password for the database user ID. For example, **maximo**.

Table 8. Common database silent installation response file properties (continued)

Category	Property	Definition
Database Configuration Automation	AUTOMATE_DB=1	Configure the automatic configuration of the database by the installation program. Set to `0` to disable. Set to `1` to enable. Either AUTOMATE_DB or DO_NOT_AUTOMATE_DB can be enabled at one time.
	DO_NOT_AUTOMATE_DB=0	Configure the automatic configuration of the database by the installation program. Set to `0` to disable. Set to `1` to enable. Either AUTOMATE_DB or DO_NOT_AUTOMATE_DB can be enabled at one time.
Remote Access Authorization	DB_RXA_USER=*user name*	Set the name of the user ID to access the remote database server system. For example, **`root`**. Only required if AUTOMATE_DB was enabled. Oracle
	DB_RXA_PASSWORD=*password*	Set a password for the remote access user ID. Only required if AUTOMATE_DB was enabled. Oracle
Database Administration	DB_INSTALL_DIR=*path*	Enter the database server installation path. For example, **UNIX** **`/opt/oracle/product/11.2.0/db_1`** **Windows** **`C:\Program Files\oracle\product\11.2.0\db_1`** Only required if AUTOMATE_DB was enabled. Oracle
	DB_ADMIN_USER=*user name*	Set the name of the database administrator. For example, **`Sys`**. Oracle
	DB_ADMIN_PASSWORD=*password*	Set a password for the remote access database administrator. Oracle
Database Table Space	DB_TABLE_SPACE_NAME=*table space name*	Set the name of the database table space. For example, **`MAXDATA`**. Oracle

Table 8. Common database silent installation response file properties (continued)

Category	Property	Definition
	DB_TABLE_SPACE_SIZE=*table space size in Mb*	Set the size of the database table space, in Mb. For example, **`5000`**. y. Only required if AUTOMATE_DB was enabled.
	DB_TEMP_TABLE_SPACE_NAME=*temporary table space name*	Set the name of the database temporary table space. For example, **`MAXTEMP`**. Oracle
	DB_TEMP_TABLE_SPACE_SIZE=*temporary table space size in Mb*	Set the size of the temporary database table space, in Mb. For example, **`1000`**. Only required if AUTOMATE_DB was enabled. Oracle
	DB_INDEX_TABLE_SPACE_NAME=*index table space name*	Set the name of the database index table space. For example, **`MAXDATA`**. Oracle
	DB_INDEX_TABLE_SPACE_SIZE=*index table space size in Mb*	Set the size of the index database table space, in Mb. For example, **`5000`**. Only required if AUTOMATE_DB was enabled. Oracle only.

Oracle silent installation properties

The following properties contain information about an Oracle database used for the deployment. These properties are only necessary if you are using an Oracle database for deployment.

Table 9. Oracle silent installation response file properties

Category	Property	Definition
Oracle	ORACLE_OWNER_ID=*user name*	Set the Oracle software owner user ID. For example, **`oracle`**. Only required if AUTOMATE_DB was enabled.
	ORACLE_OWNER_PASSWORD=*password*	Set the Oracle software owner password. Only required if AUTOMATE_DB was enabled.
	INSTANCE_LOCATION=*instance location*	Set the Oracle database instance location. For example, **`/opt/oracle/product/11.2.0/db_1`**. Only required if AUTOMATE_DB was enabled.

Common application server silent installation properties

The following properties contain common information about the application server used for the deployment.

Table 10. Common application server silent installation response file properties

Category	Property	Definition
Application Server Type	APPLICATION_SERVER_TYPE_WAS=1	Configure the application server used for the deployment. Set to **0** to disable. Set to **1** to enable. Only one Application Server Type can be enabled.

IBM WebSphere Application Server Network Deployment silent installation properties

The following properties contain information about a IBM WebSphere Application Server Network Deployment application server used for the deployment. These properties are only necessary if you are using an IBM WebSphere Application Server Network Deployment application server for deployment.

Table 11. IBM WebSphere Application Server Network Deployment silent installation response file properties

Category	Property	Definition
IBM WebSphere Application Server Network Deployment Connectivity	WAS_HOSTNAME=*host name*	Set the host name of the IBM WebSphere Application Server Network Deployment server.
	WAS_SOAP_PORT=*port*	Set the SOAP port. For example, **8879**.
Automate WebSphere Application Server Network Deployment Configuration	AUTOMATE_WAS_CLIENT=1	Automatic configuration of the WebSphere Application Server Network Deployment thin client by the Maximo Asset Management installation program. Set to **0** to disable. Set to **1** to enable.
WebSphere Application Server Network Deployment Remote Access Authorization	WAS_CLIENT_RXA_USER=*user name*	Set the name of the user ID to access the remote WebSphere Application Server Network Deployment server system. For example, **root**.
	WAS_CLIENT_RXA_PASSWORD=*passsword*	Set a password for the remote access user ID.

Table 11. IBM WebSphere Application Server Network Deployment silent installation response file properties (continued)

Category	Property	Definition
WebSphere Application Server Network Deployment Deployment Manager Configuration	WAS_HOME_DIR=*path*	Enter the installation path for WebSphere Application Server Network Deployment. For example, for UNIX, **/opt/IBM/WebSphere/AppServer** or for Windows, `C:\\Program Files\\IBM\\WebSphere\\AppServer`.
	WAS_USER=*user name*	Set the name of the user ID used to access the WebSphere Application Server Network Deployment server. For example, **wasadmin**.
	WAS_PASSWORD=*passsword*	Set a password for the WebSphere Application Server Network Deployment user ID.
	WAS_PROFILE=*profile name*	Set a name for the domain manager profile. For example, **ctgDmgr01**.
WebSphere Application Server Network Deployment Application Server Configuration	WAS_VIRTUAL_HOST_PORT=*port*	Set a port for the virtual host. For example, **80**.
	WAS_WEB_SERVER_NAME=*Web server name*	Set a name for the Web server. For example, **webserver1**.
	WAS_NODE_NAME=*node name*	Set a name for the node. For example, **ctgNode01**.
	WAS_APPLICATION_SERVER_NAME=*host name*	Set a name for the application server. For example, **MXServer**.
Integration Adapter JMS Configuration	WAS_SIB_DS_NAME=*data source name*	Set a name for the data source that is used to persist JMS messages. For example, **intjmsds**.
	WAS_JMS_PERSIST_DATASTORE=1	Persist JMS messages in a data source. Set to **0** to disable. Set to **1** to enable. Only one parameter between WAS_JMS_PERSIST_DATASTORE and WAS_JMS_DO_NOT_PERSIST_DATASTORE can be enabled.
	WAS_JMS_DO_NOT_PERSIST_DATASTORE=0	Do not persist JMS messages. Set to **0** to disable. Set to **1** to enable. Only one parameter between WAS_JMS_PERSIST_DATASTORE and WAS_JMS_DO_NOT_PERSIST_DATASTORE can be enabled.

Table 11. IBM WebSphere Application Server Network Deployment silent installation response file properties (continued)

Category	Property	Definition
DB2 Database Server Configuration	WAS_SIB_DB_SERVER_NAME=*host name*	Set the name of the system that is hosting the database used to persist JMS messages. Only required if WAS_JMS_PERSIST_DATASTORE was enabled.
	WAS_SIB_DB_SERVER_PORT=*port*	Set the access port of the database used to persist JMS messages. For example, **`50005`**. Only required if WAS_JMS_PERSIST_DATASTORE was enabled.
	WAS_SIB_DB_NAME=*database name*	Set a name for the database used to persist JMS messages. For example, **`maxsibdb`**. Only required if WAS_JMS_PERSIST_DATASTORE was enabled.
	WAS_SIB_DB_USER_NAME=*user name*	Set the name of the user ID used to access the database used to persist JMS messages. For example, **`maximo`**. Only required if WAS_JMS_PERSIST_DATASTORE was enabled.
	WAS_SIB_DB_USER_PASS=*passsword*	Set a password for the data source database user ID. Only required if WAS_JMS_PERSIST_DATASTORE was enabled.
DB2 Database Server Remote Access Authorization	WAS_SIB_DB_REMOTE_ACCESS_USER=*user name*	Set a name for the user ID used to access the remote database server used to persist JMS messages. For example, **`Administrator`**. Only required if WAS_JMS_PERSIST_DATASTORE was enabled.
	WAS_SIB_DB_REMOTE_ACCESS_PASSWORD= *passsword*	Set a password for the user ID used to access the remote database server used to persist JMS messages. Only required if WAS_JMS_PERSIST_DATASTORE was enabled.

Table 11. IBM WebSphere Application Server Network Deployment silent installation response file properties (continued)

Category	Property	Definition
DB2 Database Instance Configuration	WAS_DB_HOME_DIR=*path*	Enter the installation path for DB2. For example, for UNIX, **`/opt/IBM/db2/V9.7`** or for Windows, `C:\\Program Files\\IBM\\SQLLIB`. Only required if WAS_JMS_PERSIST_DATASTORE was enabled.
	WAS_SIB_DB_INSTANCE=*database instance name*	Set a name for the database instance used to persist JMS messages. For example, **`ctginst1`**. Only required if WAS_JMS_PERSIST_DATASTORE was enabled.
	WAS_SIB_DB_INSTANCE_ADMIN_USER=*user name*	Set a name for the administrator of the database instance used to persist JMS messages. For example, **`db2admin`**. Only required if WAS_JMS_PERSIST_DATASTORE was enabled.
	WAS_SIB_DB_INSTANCE_ADMIN_PASSWORD= *passsword*	Set a password for the administrator of the database instance used to persist JMS messages. Only required if WAS_JMS_PERSIST_DATASTORE was enabled.

Security silent installation properties

The following properties are used to configure security.

Table 12. Security silent installation response file properties

Category	Property	Definition
Security	LDAP_OPTION1=1	Configure security so that an LDAP resource is used for user authorization and authentication. Set to **0** to disable. Set to **1** to enable. Only one LDAP_OPTION parameter can be enabled at one time. If LDAP_OPTION1 is enabled, then the VMM_USER_RDN, VMM_GROUP_RDN and CREATE_DEFAULT_USERS properties are also required to have valid values.
	LDAP_OPTION2=0	Configure security so that an LDAP resource is used for user authentication only. Group management is managed from the Maximo Asset Management application. Authorization data is stored in the database. Set to **0** to disable. Set to **1** to enable. Only one LDAP_OPTION parameter can be enabled at one time.
	LDAP_OPTION3=0	Configure security so that user authentication and authorization are both managed from the Maximo Asset Management application. Authentication and authorization data is stored in the database. Set to **0** to disable. Set to **1** to enable. Only one LDAP_OPTION parameter can be enabled at one time.
	VMM_USER_RDN=*user RDN*	Set a relative distinguished name for users for VMM. For example, **ou=users,ou=SWG,o=IBM,c=US**.
	VMM_GROUP_RDN=*group RDN*	Set a relative distinguished name for groups for VMM. For example, **ou=groups,ou=SWG,o=IBM,c=US**.

Table 12. Security silent installation response file properties (continued)

Category	Property	Definition
	CREATE_DEFAULT_USERS=1	Have the Maximo Asset Management installation program create default users automatically. Set to **0** to disable. Set to **1** to enable.

Language silent installation properties

The following properties are used to configure languages.

Table 13. Language silent installation response file properties

Category	Property	Definition
Base Language	BASE_ARABIC=0	Set this language as the base language used by the Maximo Asset Management application. Set to **0** to disable. Set to **1** to enable.
	BASE_BRAZILIAN_PORTUGUESE=0	Set this language as the base language used by the Maximo Asset Management application. Set to **0** to disable. Set to **1** to enable.
	BASE_CROATIAN=0	Set this language as the base language used by the Maximo Asset Management application. Set to **0** to disable. Set to **1** to enable.

Table 13. Language silent installation response file properties (continued)

Category	Property	Definition
	BASE_CZECH=0	Set this language as the base language used by the Maximo Asset Management application. Set to **0** to disable. Set to **1** to enable.
	BASE_DANISH=0	Set this language as the base language used by the Maximo Asset Management application. Set to **0** to disable. Set to **1** to enable.
	BASE_DUTCH=0	Set this language as the base language used by the Maximo Asset Management application. Set to **0** to disable. Set to **1** to enable.
	BASE_ENGLISH=1	Set this language as the base language used by the Maximo Asset Management application. Set to **0** to disable. Set to **1** to enable.
	BASE_FINNISH=0	Set this language as the base language used by the Maximo Asset Management application. Set to **0** to disable. Set to **1** to enable.

Table 13. Language silent installation response file properties (continued)

Category	Property	Definition
	BASE_FRENCH=0	Set this language as the base language used by the Maximo Asset Management application. Set to **0** to disable. Set to **1** to enable.
	BASE_GERMAN=0	Set this language as the base language used by the Maximo Asset Management application. Set to **0** to disable. Set to **1** to enable.
	BASE_HEBREW=0	Set this language as the base language used by the Maximo Asset Management application. Set to **0** to disable. Set to **1** to enable.
	BASE_HUNGARIAN=0	Set this language as the base language used by the Maximo Asset Management application. Set to **0** to disable. Set to **1** to enable.
	BASE_ITALIAN=0	Set this language as the base language used by the Maximo Asset Management application. Set to **0** to disable. Set to **1** to enable.

Table 13. Language silent installation response file properties (continued)

Category	Property	Definition
	BASE_JAPANESE=0	Set this language as the base language used by the Maximo Asset Management application. Set to **0** to disable. Set to **1** to enable.
	BASE_KOREAN=0	Set this language as the base language used by the Maximo Asset Management application. Set to **0** to disable. Set to **1** to enable.
	BASE_NORWEGIAN=0	Set this language as the base language used by the Maximo Asset Management application. Set to **0** to disable. Set to **1** to enable.
	BASE_POLISH=0	Set this language as the base language used by the Maximo Asset Management application. Set to **0** to disable. Set to **1** to enable.
	BASE_RUSSIAN=0	Set this language as the base language used by the Maximo Asset Management application. Set to **0** to disable. Set to **1** to enable.

Table 13. Language silent installation response file properties (continued)

Category	Property	Definition
	BASE_SIMPLIFIED_CHINESE=0	Set this language as the base language used by the Maximo Asset Management application. Set to **0** to disable. Set to **1** to enable.
	BASE_SLOVAK=0	Set this language as the base language used by the Maximo Asset Management application. Set to **0** to disable. Set to **1** to enable.
	BASE_SLOVENIAN=0	Set this language as the base language used by the Maximo Asset Management application. Set to **0** to disable. Set to **1** to enable.
	BASE_SPANISH=0	Set this language as the base language used by the Maximo Asset Management application. Set to **0** to disable. Set to **1** to enable.
	BASE_SWEDISH=0	Set this language as the base language used by the Maximo Asset Management application. Set to **0** to disable. Set to **1** to enable.

Table 13. Language silent installation response file properties (continued)

Category	Property	Definition
	BASE_TRADITIONAL_CHINESE=0	Set this language as the base language used by the Maximo Asset Management application. Set to **0** to disable. Set to **1** to enable.
	BASE_TURKISH=0	Set this language as the base language used by the Maximo Asset Management application. Set to **0** to disable. Set to **1** to enable.
Additional Languages	ADD_ARABIC=0	Set this language as an additional language used by the Maximo Asset Management application. Set to **0** to disable. Set to **1** to enable.
	ADD_BRAZILIAN_PORTUGUESE=0	Set this language as an additional language used by the Maximo Asset Management application. Set to **0** to disable. Set to **1** to enable.
	ADD_CROATIAN=0	Set this language as an additional language used by the Maximo Asset Management application. Set to **0** to disable. Set to **1** to enable.

Table 13. Language silent installation response file properties (continued)

Category	Property	Definition
	ADD_CZECH=0	Set this language as an additional language used by the Maximo Asset Management application. Set to **0** to disable. Set to **1** to enable.
	ADD_DANISH=0	Set this language as an additional language used by the Maximo Asset Management application. Set to **0** to disable. Set to **1** to enable.
	ADD_DUTCH=0	Set this language as an additional language used by the Maximo Asset Management application. Set to **0** to disable. Set to **1** to enable.
	ADD_ENGLISH=0	Set this language as an additional language used by the Maximo Asset Management application. Set to **0** to disable. Set to **1** to enable.
	ADD_FINNISH=0	Set this language as an additional language used by the Maximo Asset Management application. Set to **0** to disable. Set to **1** to enable.

Table 13. Language silent installation response file properties (continued)

Category	Property	Definition
	ADD_FRENCH=0	Set this language as an additional language used by the Maximo Asset Management application. Set to **0** to disable. Set to **1** to enable.
	ADD_GERMAN=0	Set this language as an additional language used by the Maximo Asset Management application. Set to **0** to disable. Set to **1** to enable.
	ADD_HEBREW=0	Set this language as an additional language used by the Maximo Asset Management application. Set to **0** to disable. Set to **1** to enable.
	ADD_HUNGARIAN=0	Set this language as an additional language used by the Maximo Asset Management application. Set to **0** to disable. Set to **1** to enable.
	ADD_ITALIAN=0	Set this language as an additional language used by the Maximo Asset Management application. Set to **0** to disable. Set to **1** to enable.

Table 13. Language silent installation response file properties (continued)

Category	Property	Definition
	ADD_JAPANESE=0	Set this language as an additional language used by the Maximo Asset Management application. Set to **0** to disable. Set to **1** to enable.
	ADD_KOREAN=0	Set this language as an additional language used by the Maximo Asset Management application. Set to **0** to disable. Set to **1** to enable.
	ADD_NORWEGIAN=0	Set this language as an additional language used by the Maximo Asset Management application. Set to **0** to disable. Set to **1** to enable.
	ADD_POLISH=0	Set this language as an additional language used by the Maximo Asset Management application. Set to **0** to disable. Set to **1** to enable.
	ADD_RUSSIAN=0	Set this language as an additional language used by the Maximo Asset Management application. Set to **0** to disable. Set to **1** to enable.

Table 13. Language silent installation response file properties (continued)

Category	Property	Definition
	ADD_SIMPLIFIED_CHINESE=0	Set this language as an additional language used by the Maximo Asset Management application. Set to **0** to disable. Set to **1** to enable.
	ADD_SLOVAK=0	Set this language as an additional language used by the Maximo Asset Management application. Set to **0** to disable. Set to **1** to enable.
	ADD_SLOVENIAN=0	Set this language as an additional language used by the Maximo Asset Management application. Set to **0** to disable. Set to **1** to enable.
	ADD_SPANISH=1	Set this language as an additional language used by the Maximo Asset Management application. Set to **0** to disable. Set to **1** to enable.
	ADD_SPANISH=1	Set this language as an additional language used by the Maximo Asset Management application. Set to **0** to disable. Set to **1** to enable.

Table 13. Language silent installation response file properties (continued)

Category	Property	Definition
	ADD_TRADITIONAL_CHINESE=0	Set this language as an additional language used by the Maximo Asset Management application. Set to **0** to disable. Set to **1** to enable.
	ADD_TURKISH=0	Set this language as an additional language used by the Maximo Asset Management application. Set to **0** to disable. Set to **1** to enable.

Chapter 6. Programmatically verifying that the installation was successful

After you have exited the Maximo Asset Management installation program without encountering any errors, you can verify that the installation completed successfully. The installation is programmatically verified through the use of post installation validation utilities.

Before you begin

The *JAVA_HOME* environment variable must be set on the system before you can use the verification utilities.

About this task

During installation, the Maximo Asset Management installation program performs a simple health check. This health check consists of logging in to the application to verify availability. This health check might not be sufficient to verify a successful installation in all deployment scenarios. For example, if, during installation, you select the option to deploy the application EAR file at a later date, this health check cannot verify the installation. This simple health check is also insufficient for verifying an upgrade.

Post installation validation utilities are available after the product has been deployed.

The middlewareValidate utility is used to verify the middleware.

The installValidation utility is used to validate the product installation. These command-line utilities are used to verify the installation and configuration of the product in a more complete manner. These utilities can also be used to verify an existing deployment after changes in the environment, such as changes to host names, user IDs, and passwords.

Results of the installValidation utility are logged in `installValidationTrace00.log`. This log is found in the `\ibm\smp\logs` directory on the administrative workstation.

Procedure

1. Log in to the server using the user ID that was used to run the installation program. If you intend to use the installValidation utility, log in to the administrative workstation. If you intend to use the middlewareValidate utility, log in to the server hosting the middleware.
2. Ensure the *JAVA_HOME* environment variable is set properly to the location of a JRE 1.6 installation.
3. To verify product installation, from the administrative workstation, change directory to `\ibm\smp\scripts` and run the `installValidation.bat` command. For either command, use the parameters described below: To verify middleware installation, from the middleware image, update the `middleware.properties` file with the installation parameter values for middleware components to be verified, change directory to `\HealthCheck` and run the `middlewareValidate.[sh|bat]` command.

Table 14. Verification utilities parameters

Program	Syntax parameters	Input
installValidation.bat	**-action**	Use **-action** validate to start the validation of the product installation. The **-action** parameter is the only mandatory parameter when using the installValidation utility.
	-trace	Verification progress information is written to the screen during the verification process. You can modify the output using the **-tracing** parameter. • minimal Progress information is limited to error information. • normal Information includes individual test progress, individual test results, and overall progress of the entire verification process. This is the default mode of tracing. • verbose In addition to providing normal progress information, verbose tracing includes the test class name, test method name, and corrective action information.
	-confirm	You are prompted before each test is started. You must confirm each test to be performed. There is no input for this parameter.
	-component	You can provide a comma-delimited list of directories containing the test objects to limit testing to a specific set of tests. These test objects must be located in the \ibm\smp\HealthValidation\ directory. For the product installation program, only the CTGIN folder is provided.
	-dbuser	Provide the user ID used to access the database.
	-dbpwd	Provide the password of the user ID used to access the database.
	-wasuser	Provide the WebSphere Application Server Network Deployment user.
	-waspwd	Provide the password for the WebSphere Application Server Network Deployment user.
	-maxuser	Provide the Maximo Asset Management administrator user ID. For example, maxadmin.

Table 14. Verification utilities parameters (continued)

Program	Syntax parameters	Input
	-maxpwd	Provide the password for the Maximo Asset Management administrator user ID.
middlewareValidate.[sh|bat]	**-middlewareproperties**	Use **-middlewareproperties** *file* where *file* is the location of the middleware.properties file. By default, this file is found on the middleware installation media in the \HealthCheck directory. The middleware.properties contains the middleware installation properties, such as installation locations and ports. User names and passwords are not stored in this plain-text file. Some of the properties common to all platforms have been defined default values, but platform-specific properties like installation locations need to be updated in this file before starting the middlewareValidate utility. The **-middlewareproperties** parameter is the only mandatory parameter when using the middlewareValidate utility.
	-trace	Verification progress information is written to the screen during the verification process. You can modify the output using the **-trace** parameter. • minimal Progress information is limited to error information. • normal Information includes individual test progress, individual test results, and overall progress of the entire verification process. • verbose In addition to providing normal progress information, verbose tracing includes the test class name, test method name, and corrective action information. If this option is not provided, by default, no output displayed.

Table 14. Verification utilities parameters (continued)

Program	Syntax parameters	Input
	-component	Specify the middleware components: • DIRSERVER - verify installation of the optional IBM Tivoli Directory Server. • LDAPSERVER - verify configuration of the optional IBM Tivoli Directory Server. • J2EESERVER - verify installation of the WebSphere Application Server server One or more of these keywords can be specified as comma separated list. If this argument is skipped, the tool assumes all the components are selected to verify.
	-bindUser	Provide the bind user. Required to verify LDAPSERVER. The bind user credentials, bind Distinguished Name and bind password are required to be specified with the **-bindUser** and **-bindPass** options.
	-bindPass	Provide the password for the bind user. Required to verify LDAPSERVER. The bind user credentials, bind Distinguished Name and bind password are required to be specified with the **-bindUser** and **-bindPass** options.
	-wasuser	Provide the WebSphere Application Server user. WebSphere Application Server administrative user credentials are required for the LDAPSERVER and J2EESERVER component checks.
	-waspwd	Provide the password for the WebSphere Application Server user. WebSphere Application Server administrative user credentials are required for the LDAPSERVER and J2EESERVER component checks.

For example,

```
installValidation.bat -action validate
```

Results

The `installValidation.bat` validation utility results are logged in `ctginstallvalidationtrace00.log`. This log is found in the `\ibm\smp\logs` directory on the administrative workstation.

The `middlewareValidate.[sh|bat]` validation utility results are logged in `CTGInstallValidationTrace.log`. This log is found in the `HealthCheck` directory.

Chapter 7. Verifying the installation manually

After you exit the Maximo Asset Management installation program without errors, you can further verify that the installation completed successfully. The installation is manually verified by locating key artifacts and performing a few simple tasks.

Before you begin

The product installation program performs installation verification, or a health check, by logging on to the product before exiting the installation. The product installation program returns a success message if all installation steps, including the product log in task, are successful. If the health check task is unsuccessful, a `HealthCheckFailed` error is thrown for the `getUrlContentString` function. This error is in the `*install_home*\logs\CTGInstallTrace*XX*.log` file, where *XX* is a two-digit number such as 00.

About this task

To further verify that the Maximo Asset Management installation was completed successfully, perform the following verification procedures:

Procedure

1. Examine the `CTGInstallTrace00.log` file for success messages.

   The following **success** messages are found in the `CTGInstallTrace00.log` file and can be used to verify which phases of the installation were successful:

   - CTGIN2114I: The database was created successfully
   - CTGIN2135I: Tablespace maxdata created successfully
   - CTGIN2135I: Tablespace maxtemp created successfully
   - CTGIN2079I: process automation engine database configuration completed successfully (This message indicates that maxinst finished successfully.)
   - CTGIN2222I: WebSphere Application Server creation successful
   - CTGIN2188I: Creation and configuration of service integration bus successfully completed
   - CTGIN2184I: Creation and configuration of JMS resources successfully completed
   - CTGIN2310I: Application server security was successfully enabled for process automation engine
   - CTGIN2253I: buildmaximoear.cmd completed successfully
   - CTGIN2224I: Deployment of application MAXIMO was successful
   - CTGIN2253I: buildhelpear.cmd completed successfully
   - CTGIN2224I: Deployment of application MAXIMOIEHS was successful
   - CTGIN2208I: runConfigurationStep completed successfully
   - CTGIN2370I: The installation finished successfully

   If you automatically configured WebSphere Application Server Network Deployment certain messages indicate success. The following messages, found in `CTGInstallTrace00.log`, indicate that the configuration was successful:

```
<symptom>CTGIN2228I.*client</symptom>
<symptom>CTGIN2230I.*node</symptom>
<symptom>CTGIN2232I.*NodeAgent</symptom>
<symptom>CTGIN2240I.*server</symptom>
<symptom>CTGIN2238I.*security</symptom>
```

Search the `CTGInstallTrace00.log` file for the following message, which indicates that the maxinst task completed successfully:

```
CTGIN2079I, maxinst.*completed
```

2. Compare the packages chosen for installation with the packages that were installed. The Package Summary panel of the Maximo Asset Management installation program provides a summary of all the packages to be installed. You can compare the contents of that panel with a listing of what was installed on the system. Use the **`solutioninstaller`** command to list installed packages:

   ```
   install_home\bin\setupPSIenv.bat
   install_home\bin\solutionInstaller.bat -action showInstalled -type all
   ```

   The resulting list matches the packages listed in the Package Summary panel.

3. Log in to the product and verify that applications are present. Being able to log in to the product manually is a good indicator that the installation was successful. Once you have logged in, navigate through the **GoTo** menu to verify that it has been populated with the applications you expect. If you experience access problems with the product, clear the cache of your browser and try again.

Chapter 8. Configuring the HTTPOnly attribute

If applications do not start from the user interface in IBM WebSphere Application Server Network Deployment 8 environments, the problem can often be attributed to a security setting within IBM WebSphere Application Server Network Deployment. In particular, if the `HTTPOnly` attribute is set for session cookies, the applications are not accessible.

Procedure

1. Log on to the administrative console for IBM WebSphere Application Server Network Deployment.
2. From the navigation pane, browse to **Servers** > **Server Types** > **WebSphere spplication servers**.
3. Click the application server created for the product you want to update, for example, MXServer.
4. From the Configuration panel, under Container Settings, click **Session management**.
5. Under General properties, click **Enable cookies**. Do not clear this option. Click the label only.
6. Clear the **Set session cookies to HTTPOnly** check box to help prevent cross-site scripting attacks.
7. Click **OK**, save the changes, and then click **OK**.
8. Click **Save** and then click **OK**.
9. Navigate back to the Application servers table, and select the application server required.
10. Click **Restart** to restart the application server in order to apply the changes made.

Chapter 9. Post installation tasks

There are several post installation tasks required in order to complete the Maximo Asset Management deployment.

Accessing product documentation

Accessing the Maximo Asset Management information center documentation and product online help.

Important: The WebSphere Application Server deployment manager must be restarted after the installation of Maximo Asset Management. Restarting enables the full function of the information center and online help.

In order to be able to access the product documentation system with the product, complete the following steps after you install Maximo Asset Management.

1. Stop the deployment manager by running the following command:

   ```
   c:\Program Files\IBM\WebSphere\AppServer\profiles\<dmgr profile>\bin\stopManager
       -username wasadmin -password <password>
   ```

2. Start the deployment manager by running the following command:

   ```
   c:\Program Files\IBM\WebSphere\AppServer\profiles\<dmgr profile>\bin\startManager
   ```

If you manually configured the application server after you ran the product installation program, you must set the property for the product documentation server. For more information, see https://www.ibm.com/support/docview.wss?uid=swg21508594.

Important: The deployment manager (a component of WebSphere Application Server Network Deployment) allows for remote management and deployment operations. While the deployment manager is stopped, all management and deployment operations, including outside of Maximo Asset Management, are affected (stopped).

Initial data configuration

After you have successfully installed and configured Maximo Asset Management components, there are several data configuration tasks you must complete before using Maximo Asset Management.

Signing in using a default user ID

User management can be managed through the Maximo application or though the directory server you have configured to use with Maximo Asset Management

Before you begin

When first installed, Maximo Asset Management contains the following default user IDs:

Table 15. Maximo Asset Management users

User
wasadmin

Table 15. Maximo Asset Management users (continued)

User
maxadmin
mxintadm
maxreg

Important: Before you begin this procedure, if you are using a directory server as part of your deployment, ensure that these users are created in your LDAP repository.

Note: User names and passwords are case-sensitive. The defaultuser names are lowercase.

About this task

To sign in, complete the following steps:

Procedure

1. Open a browser window.
2. Navigate to the Maximo Asset Management login URL. For example: http://*host name:port*/maximo.
3. Enter the user name `maxadmin` (lower case).
4. Enter the password you entered during the installation, and click **Enter**. The default start center for maxadmin is displayed.

Configuring SMTP

Installation panels provide an opportunity to configure an SMTP server to send an administrator, or other users, e-mail notifications of system events. If you skip these panels when you install Maximo Asset Management, you can use the Maximo Asset Management interface to configure SMTP parameters.

Before you begin

This task **must** be completed before you apply changes to the database.

About this task

To configure SMTP for Maximo Asset Management, complete the following steps.

Procedure

1. Log in to the console as maxadmin.
2. Navigate to **Go To** > **System Configuration** > **Platform Configuration** > **System Properties**
3. Using the Filter feature, search for the **`mail.smtp.host`** Property Name.
4. Expand the **`mail.smtp.host`** property and set the Global Value attribute to your SMTP host.
5. Select the **`mail.smtp.host`** record check box.
6. Click the Live Refresh icon in the toolbar.
7. From the Live Refresh dialog, click **OK**.
8. Using the Filter feature, search for the **`mxe.adminEmail`** Property Name.

9. Expand the `mxe.adminEmail` property and set the Global Value attribute to your e-mail address.
10. Select the `mxe.adminEmail` record check box.
11. Click the Live Refresh icon in the toolbar.
12. From the Live Refresh dialog, click **OK**.

“Applying changes to the database” on page 124
When you create a general ledger account component, it must be applied to the Maximo database.

Create currency codes

You must define a currency code for an organization.

About this task

To define a currency code for an organization, complete the following steps.

Procedure

1. Open the Currency Code application for Users by selecting **Goto** > **Financial** > **Currency Code**
2. Click **New Row**.
3. Enter a currency name. For example, `USD`.
4. Click the **Save** icon.

Create item and company sets

You must define item and company sets for an organization.

About this task

To define item and company sets for an organization, complete the following steps:

Procedure

1. Open the Sets application for Users by selecting **Goto** > **Administration** > **Sets**.
2. Click **New Row**.
3. Enter an item name. For example, `IT Items`.
4. Enter `ITEM` in the **Type** field.
5. Click **New Row**.
6. Enter a company set name. For example, `IT Comps`.
7. Enter `COMPANY` in the **Type** field.
8. Click the **Save** icon.

Create an organization

You must define at least one organization for Maximo Asset Management.

About this task

To define an organization, complete the following steps.

Procedure

1. Open the Organizations application by selecting **Goto** > **Administration** > **Organizations**.

2. Click the **New Organization** icon in the toolbar.
3. Enter an organization name in the **Organization** field. For example, `ENGLENA`.
4. Enter the base currency you defined in the **Base Currency 1** field. For example, `USD`.
5. Enter the item set you defined in the **Item Set** field. For example, `IT Items`.
6. Enter the company set you defined in the **Company Set** field. For example, `IT Comps`.
7. Enter the default item status of `PENDING` in the **Default Item Status** field.
8. Click the**Sites** tab.
9. Click **New Row**.
10. Enter a site name in the **Site** field. For example, `B901`.
11. Click the **Save** icon.

Create a general ledger account component

You must create a general ledger account component for Maximo Asset Management.

About this task

To create a general ledger account component, complete the following steps.

Procedure

1. Open the Database Configuration application by selecting **Goto** > **System Configuration** > **Platform Configuration** > **Database Configuration**.
2. Choose the **GL Account Configuration** action.
3. Click **New Row**.
4. Enter a component name in the **Component** field. For example, `MYCOMPONENT`.
5. Enter a numeric length for the component. For example, `5`.
6. Enter a type for the component. For example, `ALN`.
7. Click **OK**.

Applying changes to the database

When you create a general ledger account component, it must be applied to the Maximo database.

About this task

To apply configuration changes to the Maximo database, complete the following steps.

Procedure

1. Log in to the Maximo console as maxadmin
2. Select **Go To** > **System Configuration** > **Platform Configuration** > **Database Configuration**. Every object that must be updated in the Maximo database has a status of To Be Added.
3. Choose the **Manage Admin Mode** action.
4. Click **Turn Admin Mode ON**, and then click **OK** when prompted. This task takes several minutes to complete. You can use the **Refresh Status** button to view progress.

5. After Admin Mode has been enabled, select **Apply Configuration Changes**, to apply the changes to the Maximo database. `To Be Changed` must not appear in the status column for objects listed.
6. Turn Admin Mode OFF.
   a. Select **Go To** > **System Configuration** > **Platform Configuration** > **Database Configuration**.
   b. Choose the **Manage Admin Mode** action.
   c. Click **Turn Admin Mode OFF**, and then click **OK** when prompted. Failing to turn off Admin Mode within the application causes cron tasks to fail.

Create a general ledger account

You must create a general ledger account for Maximo Asset Management.

About this task

To create a general ledger account, complete the following steps:

Procedure

1. Open the Chart of Accounts application by selecting **Goto** > **Financial** > **Chart of Accounts**.
2. Click the name of your organization to select it. For example, click **ENGLENA**.
3. Choose the **GL Component Maintenance** action.
4. Click **New Row**.
5. Add a GL Component value and a description and then click **OK**. For example, `1234`.
6. Click **New Row**.
7. Select your General Ledger Account.
8. Click **Save**.
9. Open the Organizations application by selecting **Goto** > **Administration** > **Organizations**\.
10. Click the organization name you created. For example, **ENGLENA**.
11. From the Clearing Account field, select the General Ledger Account you just created.
12. Select **Active**.
13. Click the **Save** icon.

Update General Ledger Component Type Authorization

You must update the general ledger component type authorization for Maximo Asset Management.

About this task

To authorize a Security Group to change a general ledge component type, complete the following steps:

Procedure

1. Open the Security Groups application by selecting **Go To** > **Security** > **Security Groups**.
2. Select the Group that provides authorization (for example, PMSCOA).

3. Click the **GL Components** tab.
4. Click the **Authorized** check box for each GL Component.
5. Click **Save**

Update Company-Related Accounts

You must update the company-related accounts for Maximo Asset Management.

About this task

To update the company-related accounts, complete the following steps:

Procedure

1. Open the Chart of Accounts application by selecting **Go To** > **Financials** > **Chart of Accounts**.
2. From the action menu, select **Company-Related Accounts**.
3. On the dialog click **New Row**.
4. Select company type 'C'.
5. Set the RBNI Account, AP Suspense Account, and AP Control Account to the components you created.
6. Click **OK**.
7. From the action menu, select **Update Database**.
8. Click **OK**.

Create default insert site

You must create a default insert site for Maximo Asset Management.

About this task

To create a default insert site, complete the following steps.

If you encounter an error message that indicates that the record is being updated by another user, log out as maxadmin and then log back in.

Procedure

1. Open the Users application by selecting **Goto** > **Security** > **Users**.
2. Search for **maxadmin** and then select it to open the record for maxadmin.
3. Enter the site you created earlier in the **Default Insert Site** field. For example, `B901`.
4. Enter the site you created earlier in the **Storeroom Site for Self-Service Requisitions** field. For example, `B901`.
5. Click **Save**.

Create worktypes

You must create worktypes for Maximo Asset Management.

About this task

To create a worktype, complete the following steps.

Procedure

1. Open the Organizations application by selecting **Goto** > **Administration** > **Organizations**.
2. Search for the organization you created. For example, **ENGLENA**.
3. Click the name of the organization to open the record for that organization.
4. Select **Work Order Options** > **Work Type** from the **Select Action** menu.
5. Click **New Row**.
6. Select a **Work Order** class.
7. Set the **Work Type** as **AR**.
8. Set **Start Status** as **INPRG**.
9. Set **Complete Status** as **COMP**.
10. Click **New Row**.
11. Select a **Work Order** class.
12. Set the **Work Type** as **UR**.
13. Set **Start Status** as **INPRG**.
14. Set **Complete Status** as **COMP**.
15. Click **New Row**.
16. Select **CHANGE** as the **Work Order class**.
17. Set the **Work Type** to a value that describes a type of change that is created. For example, you might set a **Work Type** as **MAJOR** to designate a major change. You can define as many Work Types for the CHANGE Work Order class as you would like. For example, you might define the MINOR Work Type for a minor change, and a SIG Work Type for a significant change.
18. Set **Start Status** as **INPRG**.
19. Set **Complete Status** as **COMP**.
20. Click **OK**.
21. Click **Save**.
22. Restart the MXServer application server.

Signing out and signing in

When you change a security group that includes your user ID, you must sign out and sign in to see the changes. For example, even though you have granted a group permission to create start center templates, the actions are not visible until you sign in again.

Procedure

1. Sign out.
2. Sign in as the same user.

Synchronizing users and groups

When you select application server security, the scheduled synchronization of users and groups that occurs between LDAP repositories and Maximo Asset Management is governed by the federated repositories.

Before you begin

View the cron task configuration information in the Administering section of the information center.

About this task

LDAP repositories managed by IBM WebSphere Application Server Network Deployment through Virtual Member Manager are synchronized through the VMMSYNC cron task.

To configure the synchronization schedule between LDAP repositories and Maximo Asset Management, complete the following steps:

Procedure

1. Open a web browser and point to http://*host name:port*/maximo.
2. Log in to Maximo Asset Management using the maxadmin user ID.
3. From the Maximo Asset Management interface, navigate to **Go To** > **System Configuration** > **Platform Configuration** > **Cron Task Setup**.
4. Search for the appropriate cron task in the **Cron Task** field and configure it.
5. Set the task to **active**.

What to do next

By default, the cron task performs its task every 5 minutes. Change the **Schedule** field of the cron task if you want to change the interval.

Create a maxdemo database after installation

You can create a maxdemo database and additional databases after you install Maximo Asset Management, and you can populate the database with sample data. You use the maxinst program to create additional databases.

Before you begin

The maxinst program does not provide default values for table space parameters. You must specify the data and index table space names to ensure that your installation runs smoothly.

About this task

If you created a database either automatically or manually during the installation, you can use maxinst to optionally create a maxdemo database in that database instance. If the maxinst program fails, you must recreate the Maximo database schema before running the maxinst program again.

Procedure

1. Open a command window and change directory to `C:IBM\SMP\Maximo\tools\maximo`.
2. You can create an additional database in one of the following ways:
   - To create an empty Maximo database, run the following command:
     ```
     maxinst -imaximo
     ```
   - To create a maxdemo database, run the following command:
     ```
     maxinst -stablespacename -ttablespacename
     ```

     For example, type `maxinst -sMAXIMO -tMAXIMO`.

   The system reads the `maximo.properties` file for database connectivity information. The `maximo.properties` file is in the `C:IBM\SMP\Maximo\`

Applications\Maximo\Properties directory. The system connects to the database through the JDBC connection and creates a maxdemo database.

3. You can populate the additional database by running commands with specific parameter values. The following table lists the maxinst database parameters:

Parameter	Description
-a	Database alias. If not specified, the alias mxe.db.url.property is used.
-d	Log file directory. If you are using the -l parameter, the log file is sent to the specified directory. Otherwise, the log file is sent to the log directory, for example C:\IBM\SMP\Maximo\tools\maximo\lo.
-e	Runs the SQL. This parameter is required and already present in the maxinst.bat file.
-f	File name for the properties file. If not specified, maximo.properties is used.
-i	File name of the input file (without path or extension). If not specified, the default file name Unlcvt is used.
-k	Directory of the properties file.
-l	Creates a detailed log file. This parameter is already present in the maxinst.bat file.
-o	If you are using the -l parameter, the -o parameter specifies the file name for the log file.
-p	Password for the database connection. If not specified, the mxe.db.password property or MAXIMO is used. If MAXIMO is used, it must be entered in uppercase letters.
-s	Required value: Table space for index storage.
-t	Required value: Table space for table storage.
-u	User name for database connection. If not specified, the mxe.db.user property or MAXIMO is used. If MAXIMO is used, it must be entered in uppercase letters.
-x	Required value for UNIX: Fixes the doclink file separators in UNIX environments. Note: If a UNIX environment is deployed without using this parameter, the attached documents do not function properly.

4. Add the installation-related properties to the database from the install.properties file. The install.properties file is in the C:\IBM\SMP\ETC folder. You can add these properties to the database from the System Properties application.

Understanding and configuring security

You must configure security to ensure that only authorized users can log on to Maximo Asset Management. You must also ensure that the appropriate users have access to their applications and configuration items.

The Security information contained in the Maximo Asset Management information center provides an overview of the following information:

- How security is implemented.
- The steps you perform to configure security.

Chapter 10. Uninstalling the product

Uninstalling Maximo Asset Management 7.5 is dependant upon how it was deployed.

The procedures and instructions provided here are based upon a scenario in which the Maximo Asset Management installation program has experienced an error or failure.

Maximo Asset Management uninstallation is a comprehensive procedure and does not support partial removal of individual components or process managers, including process managers deployed by other products. Process managers of previously deployed products are also removed when you uninstall Maximo Asset Management.

The Maximo Asset Management uninstallation program can only be run once. If there are errors, messages are generated that indicate conditions that you must resolve manually before attempting a reinstall. Resolution includes manually removing files from the administrative workstation.

Maximo Asset Management can only be uninstalled using the Maximo Asset Management uninstallation program as directed. Do not use other methods to attempt to uninstall Maximo Asset Management, such as using the Add/Remove Programs panel.

The uninstall procedure you follow depends on the type of Maximo Asset Management deployment you are uninstalling. For uninstallation purposes, Maximo Asset Management deployments falls into one of the following categories:

Fully-automated configuration
In this scenario, you selected the option to allow the Maximo Asset Management installation program to automatically configure middleware during deployment.

Manual configuration
In this scenario, you selected the option to manually configure middleware. You did not allow the Maximo Asset Management installation program to automatically configure middleware during deployment.

After the Maximo Asset Management uninstall process is complete, you can reinstall Maximo Asset Management by restarting the Maximo Asset Management installation program.

“Uninstalling an automatically configured deployment”
Uninstalling a Maximo Asset Management deployment that was deployed using the automatic middleware configuration options is an automated process.

“Uninstalling a manually configured deployment” on page 133
Uninstalling a Maximo Asset Management deployment that was deployed with middleware that you configured manually includes additional manual tasks.

Uninstalling an automatically configured deployment

Uninstalling a Maximo Asset Management deployment that was deployed using the automatic middleware configuration options is an automated process.

Deployments consisting of automatic middleware configuration can be uninstalled using automated methods.

Running the product uninstallation program for automatically configured middleware

Running the Maximo Asset Management uninstallation program reverts the administrative system and middleware servers back to their previous state.

Before you begin

Ensure that all applicable services are running and all middleware servers are accessible.

The Maximo Asset Management uninstallation program must be able to access the database used with Maximo Asset Management to fetch installation properties and configuration data. If the uninstallation program cannot access an unavailable, corrupted, or otherwise inaccessible database, it removes files from the administrative workstation. It then informs you that some manual recovery might be required before another Maximo Asset Management installation can be successful.

The uninstallation program uses values entered during the initial installation during uninstallation. If credentials used to access the database and J2EE server are still valid, you are not prompted to enter them again. If the uninstallation program is unable to validate these credentials you are prompted to supply the updated information. The uninstallation program would not be able to validate credentials if you updated passwords since the original installation.

Procedure

1. To run the Maximo Asset Management uninstallation program, from the administrative workstation, open a command prompt and issue the following command:
   - Windows

     ```
     install_home\_uninstall\uninstall.bat
     ```
2. From the application server information panel, enter the following information and then click **Next**.

   Remote user ID

   Enter a user ID in order to access the system hosting the application server. The remote user ID must be able to access the server using the remote access protocol enabled on that system.

   Remote password

   Enter a password for the remote user ID.

   User ID

   Enter the password for the application server administrator.

   Password

   Enter the password for the application server administrator user ID.
3. From the database administration panel, enter the information requested, and then click **Next**. For Oracle, supply credentials for the Administrator user ID and the Oracle software owner ID.
4. Review the components that are listed in the uninstallation summary panel, and then click **Uninstall**.

5. After the uninstallation process completes, specify whether you want to restart the computer now or later, and click **Done** to exit the program.
6. Remove the Maximo Asset Management installation directory, for example, `c:\ibm\smp`. You must manually remove this directory before you proceed to the reinstallation process.

Uninstalling a manually configured deployment

Uninstalling a Maximo Asset Management deployment that was deployed with middleware that you configured manually includes additional manual tasks.

Uninstalling a manually configured Maximo Asset Management deployment consists of two tasks:

- Running the Maximo Asset Management uninstallation program
- Manually dropping and recreating the database you intend to use with the reinstall process

Running the product uninstall program for manually configured middleware

Running the Maximo Asset Management uninstall program reverts the administrative system and middleware servers back to a state where you can rerun the Maximo Asset Management installation program.

Before you begin

Ensure that all applicable services are running and all middleware servers are accessible.

The Maximo Asset Management uninstall program must be able to access the database used with Maximo Asset Management to fetch installation properties and configuration data. If the uninstall program cannot access an unavailable, corrupted, or otherwise inaccessible database, it removes files from the administrative workstation. It then informs you that some manual recovery might be required before another Maximo Asset Management installation can be successful.

The uninstall program uses values entered during the initial installation during uninstall. If credentials used to access the database and J2EE server are still valid, you are not prompted to enter them again. If the uninstall program is unable to validate these credentials you are prompted to supply the updated information. The uninstall program would not be able to validate credentials if you updated passwords since the original installation.

Procedure

1. To run the Maximo Asset Management uninstall program, from the administrative workstation, open a command prompt and issue the following command:

   Windows

   ```
   install_home\_uninstall\uninstall.bat
   ```
2. From the Introduction panel, read the introductory information and then click **Next**.
3. From the application server information panel, enter the following information and then click **Next**.

User ID
Enter the password for the application server administrator.

Password
Enter the password for the application server administrator user ID.

4. Review the components that are listed in the uninstall summary panel, and then click **Uninstall**.
5. After the uninstall process has completed, click **Done** to exit the program.
6. Remove the Maximo Asset Management installation directory, for example, `c:\ibm\smp`. You must manually remove this directory before you proceed to the reinstallation process.

What to do next

You can now proceed with recovery of your manually configured database.

Database configuration recovery

Database objects created before running the Maximo Asset Management installation program must be deleted after a failed installation before the Maximo Asset Management installation program is run again.

Before rerunning the Maximo Asset Management installation program, you must drop the Maximo Asset Management database and recreate it.

Note: Alternatively, if you want to preserve the instance, you can examine the database for objects (tables, views, and procedures, for example) that were created by the maxadmin user. You can then drop those objects individually.

Restoring the Oracle database

In order to rerun the Maximo Asset Management installation program, you must first restore the Oracle database server to the same state as before Maximo Asset Management was installed.

Before you begin

The MXServer application server must be stopped before deleting the database.

About this task

Drop the Maximo Asset Management database schema user to restore the Oracle database server to its previous state. This task must be completed before you rerun the Maximo Asset Management installation program.

To restore the Maximo Asset Management database, complete the following steps:

Procedure

1. Log in to the Oracle database server as the Oracle software owner.
2. Log in to the Oracle instance with SQLPlus as a DBA user: The Oracle SID for a clean installation is ctginst1. If you are using an existing Oracle instance with Maximo Asset Management, use the Oracle SID associated with the existing instance.

   AIX, Linux, HP-UX, Solaris

   a. Set the environment variable from the command line:

```
ORACLE_SID=<your sid>
export ORACLE_SID
```

b. Start SQLPlus from the command line:

```
sqlplus /nolog
```

c. Login to SQLPlus as a DBA user:

```
connect sys/<sys password> as sysdba
```

Windows

a. Set the environment variable from the command line:

```
set ORACLE_SID=<your sid>
```

b. Start SQLPlus from the command line:

```
sqlplus /nolog
```

c. Login to SQLPlus as a DBA user:

```
connect sys/<sys password> as sysdba
```

3. Delete the Maximo Asset Management database user (maximo, by default) using an SQL command like the following sample command:

   ```
   drop user maximo cascade;
   ```

   Do not disconnect from the database. If you receive an error that you cannot drop a currently connected user, issue the following commands and use the SQL drop command:

   ```
   shutdown immediate;
   startup;
   ```

4. Manually recreate the database.

   "Manually configuring Oracle 11g" on page 55
   Use the following instructions to manually configure Oracle 11g for use with Maximo Asset Management.

   "Manually configuring Oracle 10g" on page 58
   Oracle 10g can be manually configured for use with Maximo Asset Management.

Uninstalling the product without the uninstallation program

Uninstalling the product when a failed installation does not produce an uninstallation program.

If the installation program has experienced a failure that causes it to not produce the product uninstallation program, you must perform alternative uninstallation tasks.

If uninstallation program was not produced, you must complete one of the following tasks in order to uninstall the product:

- Run the uninstallation recovery tool described in "Uninstall program recovery tool" on page 136.
- Complete the uninstallation manually using the following steps:
  1. "Recovering WebSphere Application Server configuration" on page 139.
  2. Recover the database as described in "Database configuration recovery" on page 134.
  3. Manually remove files from the system as described in "Removing files from the system" on page 142.

Uninstall program recovery tool

The uninstall program recovery tool is used to automatically uninstall Maximo Asset Management when the installation program fails to produce the product uninstallation program.

The uninstall program recovery tool is run on the administrative workstation following a failed installation. This tool performs the same functions of the Maximo Asset Management uninstallation program. This tool is intended to restore the administrative workstation and middleware servers so the Maximo Asset Management installation can be run again. The uninstall program recovery tool is available on the product media and also from the product support site.

Using the uninstallation program recovery tool

Use the uninstallation program recovery tool to restore the administrative workstation and middleware servers so the Maximo Asset Management installation can be run again.

About this task

The uninstallation program recovery tool is a command line tool that prompts you for input. This information is used as input for a collection of scripts that are run serially. These scripts perform the steps necessary to restore the administrative workstation and middleware servers so the installation program can be rerun. If you choose to skip any of the uninstallation program recovery tool tasks, you can run the tool at a later time to perform that task.

The uninstallation program recovery tool must be run on each system that hosts a component of the Maximo Asset Management deployment. For example, to remove the database associated with the deployment, you must run the program on the server hosting the database.

Procedure

1. Open a command prompt on the administrative workstation and start the uninstallation program recovery tool.
   - For Windows, use `cleanupPAE.bat`.
2. Provide input for the scripts responsible for recovering the IBM WebSphere Application Server Network Deployment server used in the deployment.
   a. Supply information for the IBM WebSphere Application Server Network Deployment used in the deployment.
      1) At the `Would you like to cleanup WebSphere Application Server? [y/n]:` prompt, select `y`.
      2) At the `Would you like to enter a custom install directory for WebSphere? [y/n]:` prompt, select `n` if you installed IBM WebSphere Application Server Network Deployment in the default directory.

         If you installed IBM WebSphere Application Server Network Deployment in a custom directory, you are prompted to enter that directory.
      3) At the `Enter your WebSphere admin user ID:` prompt, enter the user ID of the IBM WebSphere Application Server Network Deployment administrator.
      4) At the `Enter your WebSphere admin password:` prompt, enter the password of the IBM WebSphere Application Server Network Deployment administrator user ID.

b. Remove Maximo Asset Management applications from IBM WebSphere Application Server Network Deployment.

   1) At the `Would you like to remove the MAXIMO and MAXIMOIEHS applications? [y/n]:` prompt, select `y`.

      This step indicates that you want to remove both the Maximo and Maximo help applications.

   2) At the `Enter the name of the node where MAXIMO and MAXIMOIEHS are located:` prompt, enter the node associated with the Maximo and Maximo help applications.

   3) At the `Enter the name of the server where MAXIMO and MAXIMOIEHS are located:` prompt, enter the name of the web server hosting the Maximo and Maximo help applications.

   4) At the `Are you sure you want to remove the MAXIMO and MAXIMOIEHS applications? [y/n]:` prompt, select `y`.

c. Remove JMS message queue objects.

   1) At the `Would you like to remove the JMS resources? [y/n]:` prompt, select `y`.

   2) At the `Are you sure you would like to remove the JMS resources? [y/n]:` prompt, select `y`.

d. Remove Service Integration Bus objects.

   1) At the `Would you like to remove the Service Integration Bus and SIB destinations? [y/n]?` prompt, select `y`.

   2) At the `Enter the name of the node where MAXIMO was installed:` prompt, enter the node associated with the Maximo application.

   3) At the `Enter the name of the server where MAXIMO was installed:` prompt, enter the name of the web server hosting the Maximo application.

   4) At the `Are you sure you would like to remove the Service Integration Bus and SIB destinations? [y/n]:` prompt, select `y`.

e. Remove IBM WebSphere Application Server Network Deployment properties.

   1) At the `Would you like to remove the Deployment Manager custom properties? [y/n]:` prompt, select `y`.

   2) At the `Are you sure you would like to remove the Deployment Manager custom properties? [y/n]:` prompt, select `y`.

f. Remove IBM WebSphere Application Server Network Deployment environment variables.

   1) At the `Would you like to remove the WebSphere Application Server environment variables? [y/n]:` prompt, select `y`.

   2) At the `Are you sure you would like to remove the WebSphere Application Server environment variables? [y/n]:` prompt, select `y`.

g. Remove the IBM WebSphere Application Server Network Deployment virtual host.

   1) At the `Would you like to remove the Maximo Virtual Host? [y/n]:` prompt, select `y`.

   2) At the `Are you sure you would like to remove the Maximo Virtual Host? [y/n]:` prompt, select `y`.

h. Remove the IBM WebSphere Application Server Network Deployment Java Authentication and Authorization Service.

        1) At the `Would you like to remove the Java Authentication and Authorization Service (JAAS) Alias? [y/n]:` prompt, select `y`.
        2) At the `Are you sure you would like to remove the JAAS Alias? [y/n]:` prompt, select `y`.

    i. Remove IBM WebSphere Application Server Network Deployment JDBC data sources and providers.
        1) At the `Would you like to remove the JDBC data sources and providers? [y/n]:` prompt, select `y`.
        2) At the `Are you sure you would like to remove the JDBC data sources and providers? [y/n]:` prompt, select `y`.

    j. Remove IBM WebSphere Application Server Network Deployment application server custom properties.
        1) At the `Would you like to remove the application server custom properties? [y/n]:` prompt, select `y`.
        2) At the `Are you sure you would like to remove the application server custom properties?[y/n]:` prompt, select `y`.

    k. Remove users and groups.
        1) At the `Would you like to remove the Maximo users and groups? [y/n]:` prompt, select `y`.
        2) At the `Enter the Maximo administration user(Default = maxadmin):` prompt, enter the user ID.
        3) At the `Enter the Maximo system registration user(Default = maxreg):` prompt, enter the user ID.
        4) At the `Enter the Maximo system integration user(Default = mxintadm):` prompt, enter the user ID.
        5) At the `Are you sure you would like to remove the Maximo users and groups? [y/n]:` prompt, select `y`.

3. Provide input for the scripts responsible for recovering the database server used in the deployment.
    - Oracle
        a. Supply information for the database used in the deployment.
            1) At the `Would you like to cleanup the database? [y/n]:` prompt, select `y`.
            2) At the `Which database type would you like to cleanup? [DB2, Oracle, SQLServer (BAT only)]:` prompt, select Oracle.
            3) At the `Enter the SID of the Oracle instance:` prompt, enter the Oracle System ID of the Oracle instance used in the deployment.
            4) At the `Enter the Oracle install directory:` prompt, enter the Oracle installation path.

        b. Supply user information.
            1) At the `Enter the SYSDBA user:` prompt, enter the SYSDBA user ID.
            2) At the `Enter the SYSDBA password:` prompt, enter the password for the SYSDBA user ID.
            3) At the `Enter database user:` prompt, enter the Oracle database user ID.
            4) At the `Would you like to delete the <database user name> database user? [y/n]:` prompt, select `y`.

        c. Delete the Oracle table spaces and the Oracle instance.

1) At the `Would you like to delete the 'maxdata', 'maxtemp', and 'maxindex' tablespaces? [y/n]:` prompt, select `y`.

2) At the `Would you like to delete the oracle instance? [y/n]:` prompt, select `y`.

4. Provide input for the scripts responsible for recovering the administrative workstation used in the deployment.
   a. At the `Would you like to cleanup the administrator workstation? [y/n]:` prompt, select `y`.
   b. At the `Would you like to enter a custom install directory? [y/n]:` prompt, select `n` if you installed Maximo Asset Management in the default directory. If you installed Maximo Asset Management in a custom directory, you are prompted to enter that directory.
   c. At the `Are you sure you would like to cleanup the following directory: <install directory>? [y/n]:` prompt, select `y`.

Manual uninstallation

Manual uninstallation steps are sometimes necessary to uninstall Maximo Asset Management when the installation program fails to produce the product uninstallation program.

Manual uninstallation steps are performed following a failed installation. These steps are used to remove the same objects as the Maximo Asset Management uninstallation program. These steps are intended to restore the administrative workstation and middleware servers so the Maximo Asset Management installation can be run again.

Recovering WebSphere Application Server configuration

Follow these instructions to delete WebSphere Application Server objects that are created or changed by the installation program and restore WebSphere Application Server to the same state as when first installed by the middleware installation program.

About this task

As the result of a failed installation, it is possible that not all of the objects listed in these instructions were created or configured. Steps apply only to relevant objects that were created by the installation process. In addition, if you have manually created or configured WebSphere Application Server objects, you must take your own actions to ensure that they remain intact before attempting this recovery process.

Assuming that the middleware installation failure caused WebSphere Application Server to be in a nonworking state, ensure that the deployment manager and the node are running.

When you complete the WebSphere Application Server recovery process, you can proceed to the next step of the uninstall process which involves database recovery steps.

Procedure

1. Using the WebSphere Application Server administrator ID, log in to the IBM Console for WebSphere Application Server. https://<*dmgr host*>:9043/ibm/console.
2. Delete the installed Enterprise Applications:

   a. Expand **Applications**.
   b. Select **Enterprise Applications**.
   c. Select **MAXIMO** and **MAXIMOIEHS**.
   d. Click **Stop**.
   e. If not already selected, reselect **MAXIMO** and **MAXIMOIEHS**.
   f. Click **Uninstall**.
   g. Click **OK**.
3. Delete JMS resources:
   a. Delete Activation Specs
      1) Expand **Resources**.
      2) Expand **JMS**.
      3) Select **Activation specifications**.
      4) Select **intjmsact**.
      5) Click **Delete**.
   b. Delete Queues
      1) Expand **Resources**.
      2) Expand **JMS**.
      3) Select **Queues**.
      4) Select **CQIN**, **SQIN** and **SQOUT**.
      5) Click **Delete**.
   c. Delete Connection Factories
      1) Expand **Resources**.
      2) Expand **JMS**.
      3) Select **Connection factories**.
      4) Select **intjmsconfact**.
      5) Click **Delete**.
4. Delete the Service Integration Bus intjmsbus.
   a. Expand the **Service integration** link.
   b. Click **Buses**.
   c. Select the **intjmsbus** check box.
   d. Click **Delete**.
5. Remove the CTG_MAXIMO_SERVLET_URL custom property from the Deployment Manager:
   a. Expand the **System administration** link.
   b. Click **Deployment manager**.
   c. Select the Configuration tab
   d. Click **Java and Process Management**.
   e. Click **Process Definition**.
   f. Click **Java Virtual Machine (JVM)**.
   g. Click **Custom Properties**.
   h. Select the **CTG_MAXIMO_SERVLET_URL** check box.
   i. Click **Delete**.
6. Delete the CTG_MAXIMO_SERVLET_URL and ctg_JDBC_DRIVER_PATH WebSphere Application Server Environment Variables:
   a. Expand the **Environment** link.

   b. Select **WebSphere Variables**.
   c. Select **Cell=ctgCell01** from the **Scope** menu.
   d. Click **Apply**. If you have Scope set for WebSphere Application Server variables, you are not required to click **Apply** to apply changes.
   e. Select the **CTG_MAXIMO_SERVLET_URL** and **ctg_JDBC_DRIVER_PATH** check boxes.
   f. Click **Delete**.

7. Delete the Virtual Host maximo_host:
   a. Expand the **Environment** link.
   b. Select **Virtual Hosts**.
   c. Select **maximo_host**.
   d. Click **Delete**.
8. Delete the existing Java Authentication and Authorization Service (JAAS) Alias (maxJaasAlias):
   a. Expand the **Security** link.
   b. Select **Secure administration, applications, and infrastructure**.
   c. Select the Configuration tab.
   d. Select **Java Authentication and Authorization Service**.
   e. Select **J2C authentication data**.
   f. Select **maxJaasAlias**.
   g. Click **Delete**.
9. Delete created JDBC data sources:

   Delete V 4.0 data sources:

   a. Expand **Resources**.
   b. Expand **JDBC**.
   c. Select **Data sources (WebSphere Application Server V4)**.
   d. Select **DB2 Universal JDBC Driver - 4.0 XA Data Source**.
   e. Click **Delete**.

   Delete data sources:

   a. Expand **Resources**.
   b. Expand **JDBC**.
   c. Select **Data sources**.
   d. Select **DB2 Universal JDBC Driver XA Data Source** and **intjmsds**.
   e. Click **Delete**.

   Delete JDBC providers:

   a. Expand **Resources**.
   b. Expand **JDBC**.
   c. Select **JDBC providers**.
   d. Select **maxJdbcProvider**.
   e. Click **Delete**.
10. Remove added properties associated with Application server MXServer:
   a. Expand **Servers**.
   b. Select **Application servers**.
   c. Select **MXServer**.
   d. Select the Configuration tab.

   e. Expand **Java and Process Management**.
   f. Select **Process Definition**
   g. Select **Java Virtual Machine**.
   h. Select **Custom Properties**.
   i. Select **com.collation.home** and **sun.rmi.dgc.ackTimeout**.
   j. Click **Delete**.
11. Delete Maximo users:
   a. Expand **Users and Groups**.
   b. Click **Manage Users**.
   c. Click **Search** and search by user ID.
   d. Locate and select the **maxadmin**, **maxreq** and **mxintadm** user IDs, and then click **Delete**.
12. From the message dialog box, click **Save** to save all configuration changes. Ensure that you are synchronizing all changes with nodes.
13. Remove the IBM DB2 JDBC driver JAR files from the file system by deleting the `db2jcc.jar` and `db2jcc_license_cu.jar` files from the `ctgMX\lib` folder which is in the WebSphere Application Server home directory. For example, `C:\Program Files\IBM\WebSphere\AppServer`.

“Database configuration recovery” on page 134
Database objects created before running the Maximo Asset Management installation program must be deleted after a failed installation before the Maximo Asset Management installation program is run again.

Removing files from the system

If an uninstallation program is unavailable due to failed installation, product files must be manually removed from the system.

About this task

Remove files from the system by completing the following steps:

Procedure

1. Ensure that you are logged in to the system with the same user ID used to start the product installation program.
2. Manually delete the Maximo Asset Management home directory. For Windows, the default location of this directory is `C:\IBM\SMP`.

Chapter 11. Starting and stopping middleware

Use this information to start and stop middleware when necessary.

There might be occasions when you have to stop or restart middleware.

Restarting middleware on Windows

This procedure describes how to restart middleware on Windows, if you must restart any middleware services.

About this task

To properly start middleware products on Windows, use the following scripts in the order in which they are listed:

Procedure

1. Log in as a user with Administrative permissions.
2. If you installed IBM Tivoli Directory Server, start the IBM Tivoli Directory Server Admin Daemon.
   a. Click **Start**, and select **Run**.
   b. Type `services.msc`, and click **OK**.
   c. Select `IBM Tivoli Directory Admin Daemon V6.3 - idsccmdb`, and click **Start the service**.

   Alternatively, you can use the following command from the command line to start the IBM Tivoli Directory Server admin daemon:

   ```
   idsdiradm -I idsccmdb
   ```
3. If you installed IBM Tivoli Directory Server, start the IBM Tivoli Directory Server instance.
   a. Click **Start**, and select **Run**.
   b. Type `services.msc`, and click **OK**.
   c. Select `IBM Tivoli Directory Server Instance V6.3 - idsccmdb`, and click **Start the service**.

   Alternatively, you can use the following command to start the IBM Tivoli Directory Server instance:

   ```
   idsslapd -I idsccmdb
   ```

   Important: The IBM Tivoli Directory Server Instance must remain as a manual startup type. It must be started manually to synchronize correctly with the database in the context of Maximo Asset Management.
4. If you installed WebSphere Application Server, start Domain Manager
   a. Click **Start**, and select **Run**.
   b. Type `services.msc`, and click **OK**.
   c. Select `IBMWAS70Service - ctgCellManager01`, and click **Start the service**.

   Alternatively, you can use the following command from the command line to start the domain manager:

   ```
   WAS_HOME\profiles\ctgDmgr01\bin\startManager.bat
   ```

5. If you installed WebSphere Application Server, start Node
   a. Click **Start**, and select **Run**.
   b. Type `services.msc`, and click **OK**.
   c. Select `IBMWAS70Service - nodeagent`, and click **Start the service**.

   Alternatively, you can use the following command from the command line to start the node:

   ```
   WAS_HOME\profiles\ctgAppSvr01\bin\startNode.bat
   ```
6. If you installed WebSphere Application Server, start MXServer. If you created a service for starting the MXServer application server, you can use the Services control panel to start and stop it. Alternatively, you can use the following command from the command line to start the application server:

   ```
   WAS_HOME\profiles\ctgAppSrv01\bin\startServer.bat MXServer
   ```
7. If you installed WebSphere Application Server, start IBM HTTP Server and webserver1.
   a. Click **Start** and select **Run**.
   b. Type `services.msc`, and click **OK**.
   c. Select `IBM HTTP Server 7.0`, and click **Start the service**.

   Alternatively, you can type **`apache`** from the command line to start the HTTP Server.

Restarting middleware on UNIX

Middleware services on Linux and AIX platforms occasionally must be restarted, such as when a reboot occurs. Middleware servers and services must be active before running the Maximo Asset Management installation program.

About this task

To properly start middleware products on UNIX, perform the following steps:

Procedure

1. Log in as root.
2. Start servers by using the following scripts in the order in which they are listed:

   If you installed IBM Tivoli Directory Server, start IBM Tivoli Directory Server Admin Daemon

   ```
   <ITDS_HOME>/sbin/idsdiradm -I idsccmdb
   ```

   If you installed IBM Tivoli Directory Server, start IBM Tivoli Directory Server daemon

   ```
   <ITDS_HOME>/sbin/idsslapd -I <instancename>
   ```

   So this command would look like the following example:

   ```
   <ITDS_HOME>/sbin/idsslapd -I idsccmdb
   ```

   Important: The instance of IBM Tivoli Directory Server must remain as a manual startup type. It must be started manually to synchronize correctly with the database in the context of Maximo Asset Management.

   If you installed WebSphere Application Server, start Deployment Manager

   ```
   <WAS_HOME>/profiles/ctgDmgr01/bin/startManager.sh
   ```

If you installed WebSphere Application Server, start Node

```
<WAS_HOME>/profiles/ctgAppSrv01/bin/startNode.sh
```

If you installed WebSphere Application Server, start webserver1

```
<WAS_HOME>/profiles/ctgAppSrv01/bin/startServer.sh webserver1
-username <username> -password <password>
```

If you installed WebSphere Application Server, start MXServer

```
<WAS_HOME>/profiles/ctgAppSrv01/bin/startServer.sh MXServer
-username <username> -password <password>
```

If you installed WebSphere Application Server, start HTTP Server and webserver1

Linux, Solaris, HP-UX

```
/opt/IBM/HTTPServer/bin/apachectl start
```

AIX

```
/usr/IBM/HTTPServer/bin/apachectl start
```

Stopping middleware on Windows

This procedure describes how to stop the middleware on Windows , if you must stop any middleware services.

About this task

To properly stop middleware products on Windows, complete the following steps:

Procedure

1. If you installed IBM Tivoli Directory Server, stop the IBM Tivoli Directory Server Admin Daemon.
   a. Click **Start**, and select **Run**.
   b. Type `services.msc`, and click **OK**.
   c. Select `IBM Tivoli Directory Admin Daemon V6.3 - idsccmdb`, and click **Stop the service**.
2. If you installed IBM Tivoli Directory Server, start the IBM Tivoli Directory Server instance.
   a. Click **Start**, and select **Run**.
   b. Type `services.msc`, and click **OK**.
   c. Select `IBM Tivoli Directory Server Instance V6.3 - idsccmdb,`, and click **Stop the service**.
3. If you installed WebSphere Application Server, stop IBM HTTP Server and webserver1.
   a. Click **Start** and select **Run**.
   b. Type `services.msc`, and click **OK**.
   c. Select `IBM HTTP Server 7.0`, and click **Stop the service**.
4. If you installed WebSphere Application Server, start Domain Manager
   a. Click **Start**, and select **Run**.
   b. Type `services.msc`, and click **OK**.
   c. Select `IBMWAS70Service - ctgCellManager01`, and click **Stop the service**.
5. If you installed WebSphere Application Server, stop servers by using the following scripts in the order in which they are listed:

   Stop Node

   ```
   <WAS_HOME>\profiles\ctgAppSvr01\bin\stopNode.bat
   ```

Note: If this process is configured to run as a service, then stop the service:

a. Click **Start** > **Services** > **Control Panel**.

b. Click **IBM WebSphere Application Server V7.0 - nodeagent**.

c. Right click and click **Stop**.

Stop MXServer

```
<WAS_HOME>\profiles\ctgAppSrv01\bin\stopServer.bat MXServer
-username <username> -password <password>
```

Note: Unless you changed the installation locations, the following are the default values:

<HTTP_SERVER_HOME> is `C:\Program Files\IBM\HTTPServer\bin`

<WAS_HOME> is `C:\Program Files\IBM\WebSphere\AppServer`

"Configuring the WebSphere Application Server Network Deployment application server to run as a Windows service" on page 152
Configuring the WebSphere Application Server Network Deployment to run as a Windows service can make it more convenient to manage.

Stopping middleware on Linux and AIX

This procedure describes how to stop the middleware on Linux and AIX platforms, if you must stop any middleware services.

About this task

To properly stop middleware products on Linux and AIX, perform the following steps:

Procedure

1. Log in as root.
2. If you installed WebSphere Application Server, stop servers by using the following scripts in the order in which they are listed:

   If you installed DB2, stop ctginst1 instance

   ```
   su - ctginst1 -c db2stop
   ```

   If you installed IBM Tivoli Directory Server, stop IBM Tivoli Directory Server Admin Daemon

   ```
   <ITDS_HOME>/sbin/idsdiradm -h idsccmdb
   ```

   If you installed IBM Tivoli Directory Server, stop IBM Tivoli Directory Server daemon

   ```
   <ITDS_HOME>/sbin/ibmslapd -I <instancename> -k
   ```

   Important: The instance of IBM Tivoli Directory Server must remain as a manual startup type. It must be started manually to synchronize correctly with the database in the context of Maximo Asset Management.

   If you installed WebSphere Application Server, stop HTTP Server and webserver1

   Linux, Solaris, HP-UX

   ```
   /opt/IBM/HTTPServer/bin/apachectl stop
   ```

   AIX

   ```
   /usr/IBM/HTTPServer/bin/apachectl stop
   ```

If you installed WebSphere Application Server, stop Deployment Manager

```
<WAS_HOME>/profiles/ctgDmgr01/bin/stopManager.sh
```

If you installed WebSphere Application Server, stop node

```
<WAS_HOME>/profiles/ctgAppSrv01/bin/stopNode.sh -username
<username> -password <password>
```

If you installed WebSphere Application Server, stop webserver1

```
<WAS_HOME>/profiles/ctgAppSrv01/bin/stopServer.sh webserver1
-username <username> -password <password>
```

f you installed WebSphere Application Server, stop MXServer

```
<WAS_HOME>/profiles/ctgAppSrv01/bin/stopServer.sh MXServer
-username <username> -password <password>
```

Chapter 12. Advanced installation topics

This section contains information useful for advanced Maximo Asset Management deployment scenarios.

Refer to this information for installation and configuration information in advanced deployments.

WebSphere Application Server Network Deployment management

Perform these tasks if you installed WebSphere Application Server Network Deployment, or used an existing server.

Comprehensive information about running and administering can be found on the WebSphere Application Server Network Deployment support site.

Starting the application server from the command line

An application server named MXServer is created during Maximo Asset Management deployment, either manually, or automatically by the Maximo Asset Management installation program.

About this task

To start the MXServer application server from the command line, complete the following steps:

Procedure

1. Start the deployment manager:

   UNIX and Linux
   ```
   <WAS_HOME>/AppServer/profiles/ctgDmgr01/bin/startManager.sh
   ```

   Windows
   ```
   <WAS_HOME>\profiles\ctgDmgr01\bin\startManager.bat
   ```
2. Start the node:

   UNIX and Linux
   ```
   <WAS_HOME>r/profiles/ctgAppSrv01/bin/startNode.sh
   ```

   Windows
   ```
   <WAS_HOME>\profiles\ctgAppSrv01\bin\startNode.bat
   ```
3. Start the web server:

   UNIX and Linux
   ```
   <WAS_HOME>/profiles/ctgAppSrv01/bin/startServer.sh webserver1
   ```

   Windows
   ```
   <WAS_HOME>\profiles\ctgAppSrv01\bin\startServer.bat webserver1
   ```
4. Start the application server:

   UNIX and Linux
   ```
   <WAS_HOME>/profiles/ctgAppSrv01/bin/startServer.sh MXServer
   ```

   Windows
   ```
   <WAS_HOME>\profiles\ctgAppSrv01\bin\startServer.bat MXServer
   ```

Starting the application server from the administrative console

An application server named MXServer is created during Maximo Asset Management deployment, either manually, or automatically by the Maximo Asset Management installation program.

About this task

To start the MXServer application server from the administrative console, complete the following steps:

Procedure

1. Before you start the administrative console, verify that the following server processes are running. If necessary, use the commands shown from a command prompt in order to start them.

Table 16. Server processes

Server	Go To

HTTP Server	**Windows**
	`<HTTP_SERVER_HOME>\bin\apache -k start`
	`<HTTP_SERVER_HOME>\bin\apache -k stop`
	UNIX **`<HTTP_SERVER_HOME>/bin/apachectl start`**
	`<HTTP_SERVER_HOME>/bin/apachectl stop`

Deployment Manager	**Windows**
	`<WAS_HOME> \profiles\ctgDmgr01\bin\startManager.bat`
	`<WAS_HOME> \profiles\ctgDmgr01\bin\stopManager.bat`
	UNIX **`<WAS_HOME>/profiles/ctgDmgr01/bin/startManager.sh`**
	`<WAS_HOME>/profiles/ctgDmgr01/bin/stopManager.sh`

Node Agent	**Windows**
	`<WAS_HOME>\profiles\ctgAppSrv01\bin\startNode.bat`
	`<WAS_HOME>\profiles\ctgAppSrv01\bin\stopNode.bat`
	UNIX **`<WAS_HOME>/profiles/ctgAppSrv01/bin/startNode.sh`**
	`<WAS_HOME>/profiles/ctgAppSrv01/bin/stopNode.sh`

Tivoli Directory Server Instance	**Windows** 1. Click **Start**, and select **Run**. 2. Type `services.msc`, and click **OK**. 3. Select **IBM Tivoli Directory Server Instance V6.1 - idsccmdb**, and click **Start the service**. UNIX **`/ldap/V6.1/sbin/ibmslapd -I idsccmdb`**

2. To start the administrative console, open a browser window and enter the following URL: http://<*server_name*>:9060/ibm/console Where <*machine_name*> is the host name of the WebSphere Application Server Network Deployment and 9060 is the default port number for the administrative console.
3. Enter an administrative user ID and password to log in, if one is required.
4. From the administrative console, click **Servers** > **Server Types** > **Application Servers**.

5. Select the check box next to **MXServer**, the name of the WebSphere Application Server Network Deployment.
6. Click **Start**. Notice that the icon in the Status column changes to running. To stop the WebSphere Application Server Network Deployment, you can click **Stop**, which causes the icon in the Status column to change to **stopped**.

Securing the WebSphere Application Server Network Deployment administrative console

You can secure the administrative console so that only authenticated users can use it.

About this task

After enabling Virtual Member Manager for WebSphere Application Server Network Deployment security, you complete several steps to secure the console. First you identify users (or groups) that are defined in the active user registry. After you decide which users you want to access the console, you can determine their level of access by assigning roles. The roles determine the administrative actions that a user can complete. After you enable security, a user must enter a valid administrator user ID and password to access the console.

You can use the Administrative Group Roles page to give groups-specific authority to administer application servers using the administrative console. Click **Security** > **Secure administration, applications, and infrastructure** > **Administrative Group Roles** to view the available administrative group roles.

Table 17. Administrative group roles

Admin Role	Description
Administrator	Has operator permissions, configurator permissions, and the permission that is required to access sensitive data.
Operator	Has monitor permissions and can change the run time state. For example, the operator can start or stop services.
Configurator	Has monitor permissions and can change the application server configuration.
Monitor	Has the least permissions. This role primarily confines the user to viewing the application server configuration and current state.
deployer	Users granted this role can configuration and run applications.
adminsecuritymanager	Fine-grained administrative security is available using wsadmin only. However, you can assign users and groups to the adminsecuritymanager role on the cell level using wsadmin scripts and the administrative console. Using the adminsecuritymanager role, you can assign users and groups to the administrative user roles and administrative group roles. However, an administrator cannot assign users and groups to the administrative user roles and administrative group roles including the adminsecuritymanager role.
iscadmins	Has administrator privileges for managing users and groups from within the administrative console only.

Note: To manage users and groups, click **Users and Groups** in the console and then click either **Manage Users** or **Manage Groups**.

Complete the following steps to map users and groups to security roles:

Procedure

1. Select **Applications** > **Enterprise applications** > **application_name**.
2. Under Detail properties, click **Security role to user/group mapping**.
3. Select the role and click either **Look up users** or **Look up groups**. Different roles can have different security authorizations. Mapping users or groups to a role authorizes those users or groups to access applications defined by the role. Users and groups are associated with roles defined in an application when the application is installed or configured. Use the Search pattern field to display users in the Available list. Click **>>** to add users from the Available list to the Selected list.
4. Restart all the application servers.

Configuring Windows services

Creating the WebSphere Application Server Network Deployment application server and node agent to run as Windows services.

These services must be created so that they start in the correct order. Use the following procedures to create these services. First create the node agent service, then create the MXServer service.

Configuring the WebSphere Application Server Network Deployment application server to run as a Windows service

Configuring the WebSphere Application Server Network Deployment to run as a Windows service can make it more convenient to manage.

About this task

To configure the WebSphere Application Server Network Deployment application server to run as a Windows service, complete the following steps:

Procedure

1. Start the WebSphere Application Server Network Deployment administrative console by opening a browser window and entering the following URL

   `http://<server_name>:9060/ibm/console`
2. Enter an administrative user ID and password
3. Click **Servers** > **Application Servers**.
4. In the Application Servers pane, select **MXServer** and click **Start**. This action creates a server log folder used by the WASService command.
5. Select MXServer, and click **Stop**.
6. Open a command prompt window.
7. Navigate to the bin folder where you installed the Maximo application server. For example: `C:\Program Files\IBM\WebSphere\AppServer\bin`
8. Run the **`WASService`** command with the following parameters:

   serverName
   Name of Maximo application server, MXServer

   profilePath
   The profile directory of the server, for example, `C:\Program Files\IBM\WebSphere\AppServer\profiles\ctgAppSrv01`

   wasHome
   Home folder for MXServer, for example, `C:\Program Files\IBM\WebSphere\AppServer\profiles`

logRoot
Folder location of MXServer log file, for example, `C:\Program Files\IBM\WebSphere\AppServer\logs\ manageprofiles\ctgAppSrv01`

logFile
Log file name for MXServer (`startServer.log`)

restart Restarts the existing service automatically if the service fails when set to true.

9. Enter the WASService command using the following syntax:

```
WASService
-add MXServer
-serverName MXServer
-profilePath "C:\IBM\WebSphere\AppServer\profiles\ctgAppSrv01"
-wasHome "C:\IBM\WebSphere\AppServer"
-logRoot "C:\IBM\WebSphere\AppServer\profiles\ctgAppSrv01\logs\MXServer"
-logFile "C:\IBM\WebSphere\AppServer\profiles\ctgAppSrv01\logs\MXServer\
startServer.log"
-restart true
```

10. Press **Enter** after you type the **`WASService`** command, and you see a confirmation message.
11. Open a Services window and double-click **MXServer**. Then perform the following actions:
    a. Change the **Startup type** field value to **Automatic**.
    b. Click **Start** to start the service.
    c. Click **OK**.

Changing the middleware installation program configuration parameters

You can change the configuration parameters you have entered for a deployment plan *before* deploying the plan. You would use this option if you chose to cancel the deployment of the deployment plan you developed by exiting the middleware installation program. Configuration parameters for a plan can be changed only before deploying the deployment plan.

About this task

These instructions assume that you have developed a deployment plan, entered configuration parameters for the plan, and then exited the middleware installation program before actually deploying the deployment plan.

Procedure

1. Relaunch the middleware installation program from the launchpad and advance along the installation program panels until you reach the Choose Workspace panel.
2. From the Choose Workspace panel, specify the directory you previously used as the middleware installation program workspace, and then click **Next**.
3. Select **Edit the configuration parameters**, and then click **Next**.
4. Advance along the middleware installation program panels and make changes.
5. When you reach the Deployment Plan Operation panel, select **Deploy the plan**, and then click **Next**.
6. From the Deployment Plan and Parameter Configuration summary panel, review the contents of the summary, and then click **Next** to initiate the installation and configuration of the middleware you selected.

7. From the Select Middleware Image Directories panel, enter the location for compressed images for the middleware contained in the deployment plan, and a directory to use to hold the uncompressed images. After you have entered the two locations, click **Next**. During deployment, the middleware images are uncompressed onto the system.
8. Click **Finish** to exit.

Deploying EAR files

This section contains information about deploying Maximo Asset Management EAR files manually into WebSphere Application Server Network Deployment.

The following instructions are used to manually deploy the Maximo Asset Management `maximo.ear` and `maximoiehs.ear` files into WebSphere Application Server Network Deployment.

Although the Maximo Asset Management installation program deploys these EAR files when you install, there might be a few instances where it would be desirable to redeploy these EAR files manually:

- If you modify any database connection parameters in the `maximo.properties` file after the initial installation, you must rebuild of the `maximo.ear` file, and then redeploy it in WebSphere Application Server Network Deployment. In this scenario, you would likely only rebuild and redeploy the `maximo.ear` file. You would not be required to rebuild and redeploy the `maximoiehs.ear` file.
- Maximo Asset Management must be installed into a WebSphere Application Server Network Deployment application server. However, Maximo Asset Management can be run within the framework of a WebSphere Application Server Network Deployment cluster. If you want to deploy Maximo Asset Management in a cluster, you can either redeploy the Maximo Asset Management EAR files into a cluster, or, create a cluster from the application server used during the install. If you have already installed Maximo Asset Management into an application server but would like to redeploy into a cluster, then you must either uninstall the MAXIMO application ("Manually uninstalling applications from WebSphere Application Server Network Deployment" on page 155), or provide a new name for the application when installing the MAXIMO application into a cluster ("Manually installing applications in WebSphere Application Server Network Deployment" on page 155).
- If you have installed Maximo Asset Management into a development environment, you might at some point like to migrate the deployment into a test or production environment. In this scenario, you must deploy both the maximo and maximo help applications into the new environment.

  The steps outlined in "Manually installing applications in WebSphere Application Server Network Deployment" on page 155 should be performed for both applications.

Building EAR files

You can manually build Maximo Asset Management EAR files if, for example, you modify a database connection parameter in the `maximo.properties` file after the initial installation.

About this task

To manually build Maximo Asset Management EAR files, complete the following steps:

Procedure

1. Build the maximo EAR file:

   Windows
   `install_home\maximo\deployment\buildmaximoear.cmd`
2. Build the maximo help system EAR file:

   Windows
   `install_home\maximo\deployment\buildmxiehsear.cmd`

Manually uninstalling applications from WebSphere Application Server Network Deployment

This section contains information about uninstalling Maximo Asset Management applications from WebSphere Application Server Network Deployment.

Procedure

1. Log in to the WebSphere Application Server Network Deployment administrative console, select **Servers** > **Server Types** > **WebSphere application servers**, select MXServer and click **Stop**.
2. Click the Applications link.
3. Select the check box next to the application you are uninstalling. By default, the Maximo Asset Management applications are named maximo and maximoiehs.
4. Click **Uninstall**.

Manually installing applications in WebSphere Application Server Network Deployment

Maximo Asset Management applications can be added to WebSphere Application Server Network Deployment.

Procedure

1. Log on to the WebSphere Application Server Network Deployment administrative console.
2. Browse to **Applications** > **New Application** > **New Enterprise Application**.
3. From the Specify the EAR, WAR, JAR, or SAR module to upload and install page, select **Local file system**.
4. Browse to the location on your system of the `maximo.ear` file and click **Next**.
5. Select **Detailed** and then click **Next**.
6. From the Application Security Warnings panel, click **Continue**.
7. Click **Step 2: Map modules to servers**.
8. Highlight all entries listed in the Clusters and servers field, check all check boxes for Modules listed in the table, and click **Apply**.
9. Click **Step 11: Map virtual hosts for Web modules**.
10. Check all check boxes for web modules listed in the table.
11. Expand **Apply Multiple Mappings**.
12. Select a virtual host, for example, `maximo_host`, from the Virtual Host menu, and click **Apply**.
13. Click **Step 15: Map security roles to users or groups**.
14. Select the check box for `maximouser` in the Role table, and then select **Everyone** from the Map Special Subjects menu.
15. Click **Step 17: Summary**, review the summary information, and click **Finish**.

Chapter 13. Middleware on Solaris and HP-UX

Middleware versions that are not installable by the middleware installation program are installed by using graphical installation programs that are provided with each middleware product.

The procedures in this document can be used to manually install the following products on the following operating systems:

Solaris 11 SPARC and HP-UX 11i v2+3 64 bit

- IBM Tivoli Directory Server 6.3.

  IBM Tivoli Directory Server 6.3 is only supported for Solaris 11.
- IBM WebSphere Application Server Network Deployment 7
- IBM HTTP Server 7

Operating system preparation

Some operating system default configuration settings must be change to provide an environment that can host middleware operations.

The steps needed to prepare each newly supported operating system are operating system dependent.

Perform the operating system preparation steps before installing any middleware.

Installing the components

After the operating system is configured as needed, install the middleware components.

Middleware components are installed in the following order:

1. IBM Tivoli Directory Server
2. IBM WebSphere Application Server Network Deployment
3. IBM HTTP Server

Note: The media or web site you use to install middleware has directory-specific locations for each supported operating system. The directory structure is *os/product*.

These commands display the contents of the *os/product* directory.

```
cd os
ls
```

Within each *os* subdirectory are the installation directories for each middleware product.

```
ls solaris

TIV-DirectoryServer_6.3
WS-ESS_6.2.1
WS-WAS_IHS_7.0_FP15
```

```
WS-WAS_ND_7.0_Custom_FP15
WS-WAS_ND_7.0_Supplemental
WS-WAS_Plugins_7.0_FP15
WS-WAS_UpdateInstaller_7.0.0.15
```

Installing IBM Tivoli Directory Server on Solaris

You typically install IBM Tivoli Directory Server on a computer that does not host other middleware products.

Procedure

1. Login as root.
2. Copy the tar files for IBM Tivoli Directory Server to a writable disk. For Solaris, copy the `tds63-solaris-sparc-base.tar` and `tds63-solaris-sparc-gskit.tar` files from `solaris64/TIV-DirectoryServer_6.3`.
3. Unpack the files:

   ```
   tar -xvf tds63-solaris-sparc-base.tar
   tar -xvf tds63-solaris-sparc-gskit.tar
   ```
4. Change to the `/tdsV6.3/tds` directory and then type **`./install_tds.bin`**

   If you prefer, you can specify a temporary directory other than the system temporary directory. Change to the appropriate directory and type the following command at a command prompt:

   ```
   ./install_tds.bin -is:tempdir directory
   ```

   . The variable *directory* is the directory you want to use for temporary space. Be sure that you have at least 400 MB of free space in this directory. For example:

   ```
   ./install_tds.bin -is:tempdir /opt/tmp
   ```
5. When the installation wizard starts, select a language to use for the installation process, accept the license agreement, and choose a **Custom** installation.
6. Select the **Proxy Server**, **Server**, **C Client**, **Java Client**, and **Web Administration Tool** options, and then click **Next**.
7. Select **Do not specify. I will manually deploy at a later time**, then click **Next**.
8. Click **Install**.
9. Close the Instance Administration tool.
10. Click **Finish**.
11. Create the `idsccmdb` instance.
12. Start the directory server, type the following commands:
    a. `/opt/ibm/ldap/V6.3/sbin/idsdiradm -I idsccmdb`
    b. `/opt/ibm/ldap/V6.3/sbin/idsdirctl -D` *admin user ID* `-w` *admin user password*

Installing WebSphere Application Server Network Deployment

You must install WebSphere Application Server Network Deployment and create two profiles that are required at a later stage.

Procedure

1. Login as root.
2. Copy the WebSphere Application Server compressed file to a writable disk. The file is in the `WS-WAS_ND_7.0_Custom_FP15` directory.

- For Solaris, copy the WS-WAS_ND_7.0_Custom_FP15/WAS-ND_Solaris-Sparc-Custom_v7015.tar.gz file.
- For HP-UX, copy the WS-WAS_ND_7.0_Custom_FP15/WAS-ND_HpuxIA64_Custom_v7015.tar.gz file.

3. Uncompress and unpack the file:
   ```
   gzip -dfv filename.gz | tar xvf -
   ```
4. Remove the compressed files.
5. Change to the directory where you unpacked the tar file.
6. Change to the WAS directory.
7. Type `./install`
8. Proceed through the initial panels, accepting the license agreement. Accept defaults provided unless you have a specific reason to change them.
9. On the Installation directory panel, accept the default installation directory.

   The default directory is /opt/IBM/WebSphere/AppServer.

   If you change the installation directory, do not use symbolic links as the destination directory and do not add space characters to the path.
10. From the WebSphere Application Server Network Deployment environments panel, select **None** as your environment, and then click **Next**.

    Selecting **None** means that you plan to create the deployment cell, deployment manager profile, and the application server profile with the profile management tool.
11. Click **Yes** to indicate that you want to proceed.
12. Advance to the end of the installation and click **Finish**.

Creating WebSphere Application Server Network Deployment profiles

When manually installing WebSphere Application Server Network Deployment, profiles must be created before starting the Maximo Asset Management installation. The 64-bit version of WebSphere Application Server Network Deployment includes the **manageprofiles** command-line tool which you use to create profiles.

Before you begin

Ensure that you are familiar with the character limitations for commands or the shell you are using. In some cases, you might have to enter commands in order to avoid exceeding these limitations. See WebSphere Application Server Network Deployment product documentation for more information about entering lengthy commands on more than one line.

You cannot use the Profile Management tool to create WebSphere Application Server Network Deployment v7.0 profiles for 64-bit platforms. You must use the **manageprofiles** command-line tool.

About this task

The following commands can be useful for managing profiles:

Table 18. Profile commands

Task	Command
Delete a profile	*WAS_HOME*/**bin/manageprofiles.[sh|bat] -delete -profileName** *profile name*

Table 18. Profile commands (continued)

Task	Command
Refresh the profile registry (for example, after deleting a profile)	*WAS_HOME*/**bin/manageprofiles.[sh|bat] -validateAndUpdateRegistry**
List existing profiles	*WAS_HOME*/**bin/manageprofiles.[sh|bat] -listProfiles**

WAS_HOME is equal to where WebSphere Application Server Network Deployment is installed, for example, `/opt/IBM/WebSphere/AppServer/` or `C:\Program Files\IBM\WebSphere\AppServer\`

To create WebSphere Application Server Network Deployment profiles, follow these steps:

Procedure

1. Source the `setupCmdLine.[sh|bat]` script in the `bin` directory of the *`WAS_HOME`* folder to set the WebSphere Application Server Network Deployment environment to the configuration instance. *WAS_HOME* is typically in `/opt/IBM/WebSphere/AppServer` or `C:\Program Files\IBM\WebSphere\AppServer\`.
2. Create a profile ports file for the ctgDmgr01 profile. This file is used with the **`manageprofiles`** command to set the ports used by this profile.

   Note: It is important that you ensure no spaces appear after any value in this file. This circumstance can sometimes occur when cutting and pasting an example. If there is an extra space trailing any of the values WebSphere uses that space as the last character of that value. For example, you specify the value `WC_adminhost=9060`, but an extra space is typed after 9060. The value is interpreted as `WC_adminhost=9060&ltsp>` (where <sp> represents a space character).

   a. Open a new text file named `_portdef_DMgr.props` and enter the following text:

   ```
   CSIV2_SSL_SERVERAUTH_LISTENER_ADDRESS=9403
   WC_adminhost=9060
   DCS_UNICAST_ADDRESS=9352
   BOOTSTRAP_ADDRESS=9809
   SAS_SSL_SERVERAUTH_LISTENER_ADDRESS=9401
   CELL_DISCOVERY_ADDRESS=7277
   SOAP_CONNECTOR_ADDRESS=8879
   ORB_LISTENER_ADDRESS=9100
   CSIV2_SSL_MUTUALAUTH_LISTENER_ADDRESS=9402
   WC_adminhost_secure=9043
   ```

   b. Place the file in the *`WAS_HOME`* directory.
3. Create the ctgDmgr01 profile using the **`manageprofiles`** command. Type the following command, all on one line, with a space between each entry:

   ```
   WAS_HOME/bin/manageprofiles.[sh|bat]
     -create
     -templatePath  WAS_HOME/profileTemplates/dmgr
     -hostName  yourfullyqualifiedhost
     -profileName  ctgDmgr01
     -profilePath  WAS_HOME/profiles/ctgDmgr01
     -portsFile  WAS_HOME/_portdef_DMgr.props
     -cellName  ctgCell01
     -nodeName  ctgCellManager01
     -enableAdminSecurity  "false"
   ```
4. Start the ctgDmgr01 server:

```
WAS_HOME/profiles/ctgDmgr01/bin/startManager.[sh|bat]
```

5. Create a profile ports file for the ctgAppSrv01 profile. This file is used by the **`manageprofiles`** command to set the ports that are used by this profile.
   a. Open a new text file named `_portdef_AppSvr.props` and enter the following text:

      ```
      CSIV2_SSL_SERVERAUTH_LISTENER_ADDRESS=9201
      DCS_UNICAST_ADDRESS=9353
      NODE_DISCOVERY_ADDRESS=7272
      NODE_IPV6_MULTICAST_DISCOVERY_ADDRESS=5001
      BOOTSTRAP_ADDRESS=2809
      SAS_SSL_SERVERAUTH_LISTENER_ADDRESS=9901
      SOAP_CONNECTOR_ADDRESS=8878
      NODE_MULTICAST_DISCOVERY_ADDRESS=5000
      ORB_LISTENER_ADDRESS=9101
      CSIV2_SSL_MUTUALAUTH_LISTENER_ADDRESS=9202
      ```

   b. Place the file in the *WAS_HOME*directory.
6. Create the ctgAppSrv01 profile using the **`manageprofiles`** command:

   ```
   WAS_HOME/bin/manageprofiles.[sh|bat]
   -create
     -templatePath   WAS_HOME/profileTemplates/managed
     -hostName  yourfullyqualifiedhost
     -profileName ctgAppSrv01
     -profilePath WAS_HOME/profiles/ctgAppSrv01
     -cellName  ctgNodeCell01
     -nodeName ctgNode01
     -portsFile WAS_HOME/_portdef_AppSvr.props
     -dmgrHost yourfullyqualifiedhost
     -dmgrPort 8879
     -isDefault
   ```

7. Start the ctgAppSrv01 node.

   ```
   WAS_HOME/profiles/ctgAppSrv01/bin/startNode.[sh|bat]
   ```

8. Augment the ctgDmgr01 profile:

   ```
   WAS_HOME/bin/manageprofiles.[sh|bat]
     -augment
     -templatePath WAS_HOME/profileTemplates/iscae71
     -profileName ctgDmgr01
     -serverName dmgr
   ```

9. Restart servers.

   ```
   WAS_HOME/profiles/ctgDmgr01/bin/stopManager.[sh|bat]
   WAS_HOME/profiles/ctgDmgr01/bin/startManager.[sh|bat]
   WAS_HOME/profiles/ctgAppSrv01/bin/stopNode.[sh|bat]
   WAS_HOME/profiles/ctgAppSrv01/bin/startNode.[sh|bat]
   ```

10. Start `firststeps.[sh|bat]` and select the Installation Verification option to confirm that your server has been properly installed and started.

    ```
    WAS_HOME/profiles/ctgDmgr01/firststeps/firststeps.[sh|bat]
    ```

"Manually configuring Virtual Member Manager on WebSphere Application Server Network Deployment"
Some deployment environments require the manual configuration of Virtual Member Manager to secure Maximo Asset Management.

Manually configuring Virtual Member Manager on WebSphere Application Server Network Deployment

Some deployment environments require the manual configuration of Virtual Member Manager to secure Maximo Asset Management.

Before you begin

For a review of Maximo Asset Management security options, see the security planning information in this document.

Important: Before you begin this procedure, ensure that you have a wasadmin user created in your LDAP repository.

If you intend to configure Virtual Member Manager to use SSL with a federated LDAP repository, it must be done only after a successful Maximo Asset Management installation. If Virtual Member Manager is configured to use SSL with a federated LDAP repository before completing the Maximo Asset Management installation, the installation fails. Do not configure a Virtual Member Manager LDAP federated repository to use SSL with an LDAP directory before installing Maximo Asset Management. Configure SSL after the Maximo Asset Management installation program has completed successfully.

About this task

During the installation process, the Maximo Asset Management installation program provided you with the option of automatically configuring Maximo Asset Management middleware. If you elected to have the Maximo Asset Management installation program automatically configure Maximo Asset Management middleware, then it will, among other tasks, perform Virtual Member Manager configuration for you. If you elected to manually configure Maximo Asset Management middleware for use with Maximo Asset Management, you must manually configure Virtual Member Manager.

Virtual Member Manager provides you with the ability to access and maintain user data in multiple repositories, and federate that data into a single virtual repository. The federated repository consists of a single named realm, which is a set of independent user repositories. Each repository can be an entire external repository or, in the case of LDAP, a subtree within that repository. The root of each repository is mapped to a base entry within the federated repository. The root is a starting point within the hierarchical namespace of the virtual realm.

To add an LDAP directory to the Virtual Member Manager virtual repository, you must first add the LDAP directory to the list of repositories available for configuration for the federated repository. You must then add the root of baseEntries to a search base within the LDAP directory. Multiple base entries can be added with different search bases for a single LDAP directory.

The values provided here are example purposes only. If you are using IBM Tivoli Directory Server, enter the values used during the installation and configuration of IBM Tivoli Directory Server. If you are configuring Virtual Member Manager to use Microsoft Active Directory, substitute values where appropriate in this procedure. You must modify the VMMCRONTASK accordingly.

To add the IBM Tivoli Directory Server or Microsoft Active Directory to VMM, complete the following steps:

Procedure

1. Start the WebSphere Application Server Network Deployment application server.

2. Start Internet Explorer and open the WebSphere Application Server Network Deployment administrative console by typing the following URL:

   ```
   http://<server_name>:<port_number>/ibm/console
   ```

   For example, enter a URL like the following sample URL:

   ```
   http://localhost:9060/ibm/console
   ```

3. At the login screen, enter your user ID, then click **Log in**. This action opens the Welcome screen for the WebSphere Application Server Network Deployment administrative console.
4. Select **Security** > **Secure administration, applications, and infrastructure**.
5. Locate the User account repository area and pick **Federated repositories** from the Available realm definition field, and then click **Configure**.
6. Click **Manage repositories**, located under Related Items.
7. Click **Add** to create new repository definition under the current default realm.
8. Enter the following values, click **Apply**, and then click **Save**.

   Repository identifier
   For IBM Tivoli Directory Server, enter `ISMITDS`.

   Directory type
   For IBM Tivoli Directory Server, select `IBM Tivoli Directory Server`.

   Primary host name
   Enter the fully qualified host name or IP address of the directory server.

   Port Enter `389`.

   Support referrals to other LDAP servers
   Set this value to `ignore`.

   Bind distinguished name
   For IBM Tivoli Directory Server, enter `cn=root`.

   Bind password
   Enter the password for the bind distinguished name.

   Login properties
   Leave this value blank.

   Certificate mapping
   Select **EXACT_DN**

9. Return to the Federated repositories panel by clicking **Security** > **Secure administration, applications, and infrastructure**, selecting **Federated repositories** from the Available realm definitions menu, and then clicking **Configure**.
10. Locate the Repositories in the realm area and click **Add Base entry to Realm**. If there is an existing file repository entry in the Repositories in the realm table, you must select it click **Remove**. Save the change after creating the entry.
11. Enter the following values, click **Apply**, and then click **Save**.

    Repository
    For IBM Tivoli Directory Server, select `ISMITDS`.

    Distinguished name of a base entry that uniquely identifies this set of entries in the realm
    For IBM Tivoli Directory Server, enter `ou=SWG,o=IBM,c=US`.

Distinguished name of a base entry in this repository
For IBM Tivoli Directory Server, enter `ou=SWG,o=IBM,c=US`.

12. From the Federated repositories configuration area, enter the following values, click **Apply**, and then click **Save**:

    Realm name
    Enter `ISMRealm`.

    Primary administrative user name
    Enter `wasadmin`. This value must be a valid user from the configured LDAP repository.

    Server user identity
    Select **Automatically generated server identity**.

    Ignore case for authorization
    Select this check box.

13. Click **Supported entity types**, and then click **PersonAccount**.
14. From the PersonAccount configuration area, enter the following values:

    Entity type
    Verify that the value is **PersonAccount**.

    Base entry for the default parent
    For IBM Tivoli Directory Server, enter `ou=users,ou=SWG,o=IBM,c=US`.

    Relative Distinguished Name properties
    Enter `uid`.

15. Click **OK** and then click **Save**.
16. Click **Supported entity types**, and then click **Group**.
17. From the Group configuration area, enter the following values:

    Entity type
    Verify that the value is **Group**.

    Base entry for the default parent
    For IBM Tivoli Directory Server, enter `ou=groups,ou=SWG,o=IBM,c=US`.

    Relative Distinguished Name properties
    Enter `cn`.

18. Click **OK** and then click **Save**.
19. Click **Supported entity types**, and then click **OrgContainer**.
20. From the OrgContainer configuration area, enter or verify the following values:

    Entity type
    Verify that the value is **OrgContainer**.

    Base entry for the default parent
    For IBM Tivoli Directory Server, enter `ou=SWG,o=IBM,c=US`.

    Relative Distinguished Name properties
    Enter `o;ou;dc;cn`.

21. Click **OK** and then click **Save**.
22. Browse to **Security** > **Secure administration, applications, and infrastructure**.
23. From the Secure administration, applications, and infrastructure configuration page, complete the following:
    a. Enable **Enable administrative security**.
    b. Enable **Enable application security**.

c. Clear the option for **Use Java 2 security to restrict application access to local resources**.

d. From Available realm definition, select **Federated repositories**.

e. Click **Set as current**.

24. Click **Apply**, and then click **Save**.

25. Restart WebSphere Application Server Network Deployment and the managed nodes by running the following commands:

    a. `<WAS_HOME>\profiles\ctgDmgr01\bin\stopManager.bat`

    b. `<WAS_HOME>\profiles\ctgAppSrv01\bin\stopNode.bat`

    c. `<WAS_HOME>\profiles\ctgDmgr01\bin\startManager.bat`

    d. `<WAS_HOME>\profiles\ctgAppSrv01\bin\startNode.bat`

    Note: Substitute UNIX path and file extension values where appropriate.

"Performing WebSphere Application Server Network Deployment configuration tasks" on page 65
Use this procedure to perform WebSphere Application Server Network Deployment configuration tasks.

Installing the WebSphere update installer

This procedure uses the update installer to apply maintenance. \

Before you begin

Complete documentation for the update installer is at http://publib.boulder.ibm.com/infocenter/wasinfo/v6r1/index.jsp?topic=/com.ibm.websphere.base.doc/info/aes/ae/tins_updi_install.html. Review the prerequisites before you install the update installer.

About this task

The update installer simplifies maintenance of WebSphere Application Server Network Deployment and related components. These components include things such as the HTTP server plug-in and fix packs.

Procedure

1. Copy the update installer compressed file to a writable disk. The file is in the `WS-WAS_UpdateInstaller_7.0.0.15` directory.
   - For Solaris, copy the `7.0.0.15-WS-UPDI-SolarisSparc64.tar.gz` file.
   - For HP-UX, copy the `7.0.0.15-WS-UPDI-HpuxIA64.tar.gz` file.
2. Uncompress the file. Type `unzip` *`fileName`*`.zip`.
3. Change to the directory that contains the uncompressed files and type **`./install`**.
4. Accept the license agreement.
5. The default installation directory is `opt/IBM/WebSphere/UpdateInstaller`. Change this value if required; otherwise accept the default location.
6. Before you finish the installation, clear the option to **Launch IBM Update Installer for WebSphere software on exit**.

Installing and configuring IBM HTTP Server

This procedure provides task information for manually installing and configuring IBM HTTP Server.

Procedure

1. Log on as root, on the system where you installed WebSphere Application Server Network Deployment.
2. Log in to the administrative console. Ensure the ctgDmgr01 deployment manager is running and that the SOAP port is set to listen at the correct port (8879 is the default).

   If the deployment manager must be started, use the following command:

   ```
   <WAS_HOME>/profiles/ctgDmgr01/bin/startManager.sh
   ```
3. Copy the IBM HTTP Server compressed file to a writable disk.

   For Solaris
   Copy `solaris64/WS-WAS_ND_7.0_Supplemental/C1G3IML.tar.gz`

   For HP-UX
   Copy `hpux-ia64/WS-WAS_ND_7.0_Supplemental/C1G2XML.tar.gz`
4. Uncompress the `C1G3IML.tar.gz` or `C1G2XML.tar.gz` file.
5. Extract the contents of the `C1G3IML.tar` or `C1G2XML.tar` file.
6. Change to the `IHS` directory and start the installation program:

   ```
   ./install
   ```
7. From the Welcome panel, click **Next**.
8. Accept the license agreement and click **Next** to display the installation root directory panel.
9. From the System prerequisites check panel, click **Next**.
10. Specify the installation location, the default is `/opt/IBM/HTTPServer`, and click **Next**.
11. From the Port Values Assignment panel, specify the following values, and click **Next**.

    HTTP Port
    80

    HTTP Administration Port
    8008
12. From the HTTP Administration Server Authentication panel, specify the following values, and click **Next**.

    Create a user ID for IBM HTTP administration server authentication
    Enable this option by selecting this check box.

    User ID
    Specify `wasadmin`

    Password
    Specify the password for the wasadmin user.
13. From the Setup HTTP Administration Server panel, specify the following values, and click **Next**.

    Set up IBM HTTP administration server to administer IBM HTTP Server
    Enable this option by selecting this check box.

    Create a unique user ID and group for IBM HTTP Server administration
    Enable this option by selecting this check box.

    User ID
    Specify `wasadmin`.

    Group Specify `ihsadmin`

14. From the IBM HTTP Server plug-in for WebSphere Application Server panel, specify the following values, and click **Next**.

    Install the IBM HTTP Server plug-in for IBM WebSphere Application Server
    Enable or clear this check box to disable this option as is appropriate for your configuration. In an environment where you have multiple deployment manager profiles, it is more practical to run the web server plug-ins installation task separately. This task is done by running the plug-in installation program after exiting the IBM HTTP Server installation program. However, if your WebSphere environment only contains a single deployment manager profile, you can leave the WebSphere plug-in option selected. When it is selected, the web server plug-ins installation task starts when you click **Next**.

    If you decide to install the IBM HTTP Server plug-in now, you must configure it. Perform the following steps to configure the plug-in.

    a. Stop and start the deployment manager:

       `WAS_HOME/profiles/ctgDmgr01/bin/stopManager.sh`

       `WAS_HOME/profiles/ctgDmgr01/bin/startManager.sh`

    b. Copy the `/opt/IBM/HTTPServer/Plugins/bin/configurewebserver1.sh` file to `WAS_HOME/bin/`

    c. Change directory to `WAS_HOME/bin` and then use the following command:

       ```
       ./configurewebserver1.sh
       ```

    d. Start the IBM HTTP Server servers:

       ```
       /opt/IBM/HTTPServer/bin/adminctl start
       /opt/IBM/HTTPServer/bin/apachectl start
       ```

    e. Log in to the WebSphere administrator console and ensure that webserver1 has started.

    http://publib.boulder.ibm.com/infocenter/wasinfo/v7r0/index.jsp?topic=/com.ibm.websphere.ihs.doc/info/welcome_ihs.html

Installing IBM HTTP Server fix packs:

IBM HTTP Server fix pack must be installed. This fix pack updates the base installation of the IBM HTTP Server to the latest maintenance level.

Procedure

1. Copy the fix pack file to the `/opt/IBM/HTTPServer/maintenance` directory. Create this directory if it does not exist.
   - For Solaris, copy the `solaris/WS-WAS_IHS_7.0_FP15/7.0.0-WS-IHS-SolarisSparc64-FP0000015.pak` file.
   - For HP-UX, copy the `hpux-ia64/WS-WAS_IHS_7.0_FP15/7.0.0-WS-IHS-HpuxIA64-FP0000015.pak` file.
2. Stop IBM HTTP Server. Type `/opt/IBM/HttpServer/bin/apachectl stop`.
3. Stop the admin server. Type `/opt/IBM/HttpServer/bin/adminctl stop`.
4. Stop WebSphere Application Server and the managed nodes using the following commands.

   a. *WAS_HOME*/profiles/ctgAppSrv01/bin/stopNode.sh

   b. *WAS_HOME*/profiles/ctgDmgr01/bin/stopManager.sh
5. Install the fix pack.

   a. Start the update installer wizard:

      ```
      /opt/IBM/WebSphere/UpdateInstaller/update.sh
      ```

b. Click **Next**.

c. From the Product Selection panel, select the IBM HTTP Server directory by browsing to the `/opt/IBM/HTTPServer` directory, and then clicking **Next**.

d. From the Maintenance Operation Selection panel, select **Install maintenance package,** and then click **Next**.

e. From the Maintenance Package Directory Selection panel, browse to the `/opt/IBM/HTTPServer/maintenance` directory, and then click **Next**.

f. From the Available Maintenance Package to Install panel, click **Select Recommended Updates**, select the target update, and click **Next**.

g. On the Installation Summary screen, click **Next** to begin the installation of the critical fixes.

6. Start IBM HTTP Server. Type `/opt/IBM/HTTPServer/bin/apachectl start`.
7. Start the admin server. Type `/opt/IBM/HTTPServer/bin/adminctl start`.
8. Restart WebSphere Application Server and the managed nodes:

   a. *WAS_HOME*/profiles/ctgDmgr01/bin/startManager.sh

   b. *WAS_HOME*/profiles/ctgAppSrv01/bin/startNode.sh

Installing the WebSphere plug-in

This procedure provides task information for manually installing and configuring WebSphere plug-in for IBM HTTP Server. This procedure is optional if you chose to install and configure the WebSphere plug-in when you installed the IBM HTTP Server.

Procedure

1. Logon as root to the system where you WebSphere is installed.
2. Change to the directory where you previously extracted the `C1G3IML` or `C1G2XML` tar file (when you installed IBM HTTP Server). For example, for Solaris, this path might be `solaris64/WS-WAS_ND_7.0_Supplemental/plugin`.
3. Change to the `plugin` directory.
4. From a command line, start the WebSphere plug-in installation program.

   ```
   ./install
   ```
5. On the Welcome panel, clear the option to learn more about the **Installation roadmap: Overview and installation scenarios**. Click **Next**.
6. Accept the license agreement and click **Next**.
7. From the plug-in selection panel, select the IBM HTTP Server V7 plug-in, and then click **Next**.
8. From the installation scenario panel, select **WebSphere Application Server machine (local)**, and then click **Next**.
9. Accept or change the installation directory; the default is `/opt/IBM/HTTPServer/Plugins` because you chose to install after exiting the installation for IBM HTTP Server. Click **Next**.
10. Specify the location where you installed the application server; the default is `/opt/IBM/WebSphere/AppServer`. Click **Next**.
11. From the select profile panel, select `ctgDmgr01` from the list, and then click **Next**.
12. From the web server configuration file panel, specify the following information:

    Select the existing IBM HTTP Server httpd.conf file

    Browse to the location of the `httpd.conf` file; the default is `/opt/IBM/HTTPServer/conf/httpd.conf`.

Specify the Web server port
The default is port 80.

Clicking **Next** might produce warning message that indicates that the selected IBM HTTP Server configuration file already contains plug-in entries. If you proceed, this configuration file is updated with a new `plugin-cfg` xml file location. You can click **OK** to proceed.

13. From the web server definition panel, specify a unique web server definition name; the default name (webserver1) is satisfactory.
14. Accept the default web server plug-in configuration file name (`plugin-cfg.xml`) and location.
15. Click **Next** to acknowledge the manual configuration steps.
16. From the installation summary panel, click **Next**.
17. When the installation is complete, click **Finish**.
18. Stop and start the deployment manager:

    ```
    WAS_HOME/profiles/ctgDmgr01/bin/stopManager.sh
    WAS_HOME/profiles/ctgDmgr01/bin/startManager.sh
    ```

19. Copy the `/opt/IBM/HTTPServer/Plugins/bin/configurewebserver1.sh` file to *WAS_HOME*`/bin/`
20. Change directory to `<`*WAS_HOME*`>/bin` and then run the following command:

    ```
    ./configurewebserver1.sh
    ```

21. Start the IBM HTTP Server servers:

    ```
    /opt/IBM/HTTPServer/bin/adminctl start
    /opt/IBM/HTTPServer/bin/apachectl start
    ```

22. Login to the WebSphere administrator console and ensure that webserver1 is started.

Installing WebSphere Application Server Network Deployment plug-in fix packs:

The WebSphere Application Server Network Deployment plug-in fix pack 17 is required. This task updates the base installation of the plug-in to the latest maintenance level.

Procedure

1. Copy the fix pack file to the `/opt/IBM/WebSphere/UpdateInstaller/maintenance` directory. Create this directory if it does not exist.
   - For Solaris, copy the `solaris64/WS-WAS_Plugins_7.0_FP17/7.0.0-WS-PLG-SolarisSparc64-FP0000017.pak` file.
   - For HP-UX, copy the `hpux-ia64/WS-WAS_Plugins_7.0_FP17/7.0.0-WS-PLG-HpuxIA64-FP0000017.pak` file.
2. Stop the IBM HTTP Server. Type `/opt/IBM/HTTPServer/bin/apachectl stop`.
3. Stop WebSphere Application Server Network Deployment and the managed nodes. Use the following commands.
   a. *WAS_HOME*`/profiles/ctgAppSrv01/bin/stopNode.sh`
   b. *WAS_HOME*`/profiles/ctgDmgr01/bin/stopManager.sh`
4. Install the fix pack.
   a. Launch the update installer wizard:

      ```
      /opt/IBM/WebSphere/UpdateInstaller/update.sh
      ```

   b. Click **Next**.

c. From the Product Selection panel, select the IBM HTTP Server `Plugin` directory by browsing to the `/opt/IBM/HTTPServer/Plugin` directory, and then clicking **Next**.
d. From the Maintenance Operation Selection panel, select Install maintenance package, and then click **Next**.
e. From the Maintenance Package Directory Selection panel, browse to the `/opt/IBM/WebSphere/UpdateInstaller/maintenance` directory, and then click **Next**.
f. From the Available Maintenance Package to Install panel, click **Select Recommended Updates**, select the target update, and click **Next**.
g. On the Installation Summary screen, click **Next** to begin the installation of the critical fixes.

5. Start the IBM HTTP Server. Type `/opt/IBM/HTTPServer/bin/apachectl start`
6. Restart WebSphere Application Server Network Deployment and the managed nodes:
   a. `WAS_HOME/profiles/ctgDmgr01/bin/startManager.sh`
   b. `WAS_HOME/profiles/ctgAppSrv01/bin/startNode.sh`

Configuring Virtual Member Manager on IBM WebSphere Application Server Network Deployment

Virtual Member Manager (VMM) provides you with the ability to access and maintain user data in multiple repositories. You can also federate that data into a single virtual repository.

Before you begin

Before configuring VMM, you might consider creating a system backup image. Having a backup allows you to restore the system to a pre-VMM state. If you chosoe to relocate your LDAP data in the future, you can reconfigure VMM to use a different LDAP server

About this task

See “Manually configuring Virtual Member Manager on WebSphere Application Server Network Deployment” on page 161 to add an IBM Tivoli Directory Server repository to VMM. This task is required and must be performed.

The federated repository managed by VMM consists of a single named realm, which is a set of independent user repositories. Each repository can be an entire external repository or, in the case of LDAP, a subtree within that repository. The root of each repository is mapped to a base entry within the federated repository. The root is a starting point within the hierarchical namespace of the virtual realm.

Procedure

1. To add an LDAP directory to the VMM virtual repository, you must first add the LDAP directory to the list of repositories. This list consists of the repositories that are available for configuration for the federated repository.
2. Add the root of baseEntries to a search base within the LDAP directory. Multiple base entries can be added with different search bases for a single LDAP directory.

Chapter 14. Backup and restoration

Like all important business data, it is a good idea to establish a process and schedule for backing up Maximo Asset Management data.

Back up and restore middleware application data using the methods described in the documentation for that product is important. Also, establish a process for backing up data contained on the Maximo Asset Management administrative workstation.

The default installation directory on the Maximo Asset Management administrative workstation is `C:\ibm`. This directory contains the critical files for your Maximo Asset Management deployment, which includes all class files and customizations that have been performed in your environment, the current Enterprise Archive (EAR) file, and the properties files and installation tools used for your environment. Plan to back up Maximo Asset Management administrative workstation data just after initial deployment and schedule periodic backups on an ongoing basis.

Backing up the administrative workstation

It is recommended that you back up all Maximo Asset Management middleware applications and Maximo Asset Management administrative workstation on a regular basis.

About this task

The default installation directory on the administrative workstation is `C:\ibm`. This directory contains the critical files for your Maximo Asset Management deployment.

Specifically, the administrative workstation contains the following items:

- Class files and customizations performed in your environment.
- The current Enterprise Archive (EAR) file that was deployed to the application server..
- The properties files and installation tools used for your environment.

It is important to make a back up of the database at the same time that you back up the administrative workstation. During restoration, you restore the database back up at the same time you restore the administrative workstation back up it was paired with.

To back up critical Maximo Asset Management information, complete the following steps:

Procedure

1. Back up the Maximo Asset Management database, J2EE server, and authentication server information using the instructions provided by your middleware vendors.
2. Create a backup of the installation directory. By default, this directory is `C:\IBM\SMP`. Ensure that all file permissions are preserved.

Restoring the administrative workstation

This section details how to restore previously backed up Maximo Asset Management administrative workstation information to a Windows workstation. This information can be used to return an existing Maximo Asset Management administrative workstation to a previous state.

Before you begin

It is important to restore the back up of the database that was made when you backed up the administrative workstation. A database back up should be restored with the administrative workstation back up it was paired with.

About this task

To restore Maximo Asset Management information to an administrative workstation, complete the following steps:

Procedure

1. Restore the database back up that was paired with the administrative workstation back up you are restoring.
2. Log on to the target administrative system with the same user ID that was used to install the product on the existing administrative workstation.
3. Copy the Maximo Asset Management installation files and directories to the file system of the target administrative system. You must maintain the directory structure of the original installation. For example, if the Maximo Asset Management installation directory on the existing administrative system is `C:\IBM\SMP`, you cannot copy those files to a `C:\NewAdminWS\IBM\SMP` directory on the target administrative workstation.

Installation properties

Installation properties are recorded in properties files during a deployment and are used as input by future install-related actions. Installation properties are found in the `install.properties` and `maximo.properties` files as well as the database. You should only modify properties found in the `install.properties` file that are related to host names or user IDs. Changing values for other properties can severely impact your ability to perform future installation actions, upgrades and fix pack installations.

Table 19. Installation properties

Category	Property	Definition
MAXIMO Properties	Maximo.InstallLocation	Install location of the maximo directory. For example, `C:\\IBM\\SMP\\maximo`
	mxe.db.user	Database user that the server uses to attach to the database server. For example, `maximo`
	mxe.db.schemaowner	Owner of the database schema. For example, `maximo`
	mxe.db.password	Password for the database user name.
	mail.smtp.host	SMTP host server.

Table 19. Installation properties (continued)

Category	Property	Definition
	mxe.workflow.admin	E-mail account of the workflow administrator.
	mxe.adminEmail	Valid e-mail address used by workflows to communicate with workflow participants.
	mxe.name	Name to bind the MXServer server object to in the RMI registry. For example, `mxserver`.
	mxe.hostname	Name of the machine and port hosting MXServer.
	mxe.rmi.port	RMI communication port. If set at zero, RMI uses any available port. You can select another available port number.
	mxe.registry.port	The port number used to bind RMI/JRMP communications. For example, `13400`. The RMI registry is started by the first instance of the maximo application to run. An environment could have multiple instances of the product application running. This registry coordinates these instances. There is a single central RMI registry server. This value is the port available for the other application instances to communicate with the central server.
	mxe.allowLocalObjects	Set to true in production environments, to improve system performance. Set to false for development work, or for custom applications. The default is `false`.
	mxe.useAppServerSecurity	Indicates whether to use LDAP or native authentication. Setting this value to 1 indicates you are using LDAP for security.
	mxe.MLCacheLazyLoad	By default, the multi-language metadata cache loads one object at a time. Set this flag to 1 to load all objects simultaneously for one language.
	mxe.UserLicenseKey	The product enabler (license key) is used during installation. If the product enabler changes this value must be updated.
	mxe.adminuserid	The administrative user. Used by the server for administrative tasks and to run cron tasks. This user must have access to all Sites in the system.
	mxe.adminuserloginid	Defines the default login user ID for the product application. The default value is `maxadmin`.
	mxe.adminPasswd	The password for the mxe.adminuserloginid user.

Table 19. Installation properties (continued)

Category	Property	Definition
	mxe.system.reguser	Self registration user. This user is responsible for the process by which users can create their own accounts. The default value is `maxreg`.
	mxe.system.regpassword	User registration login password. This value is the password for the user listed for mxe.system.reguser.
	mxe.email.charset	The character set for e-mail notifications sent from the product. When this property is defined, it is the charset that is used to encode the subject and message when an e-mail notification is sent.
	mxe.reorder.previewtimeout	The reorder preview time out period (in minutes). This value must be set to the same value as the Web server session time out. The default value is `30` minutes.
	mxe.security.provider	The security provider is obtained from the policy file, which is normally `com.sun.crypto.provider.SunJCE`. To use a different provider, you can specify a value for this parameter.
	mxe.mbocount	Displays the number of business objects created by the server. The default is 1. Changing the value to `0` disables this feature.
	mxe.esig.defaultuserid	Set this flag to `true` if you want the Esignature login dialog to default to the login ID. The default value is `true`.
	maximo.min.required.db.version	Defines what the minimum level of database is required for an upgrade. An example value would be `7100`.
	mxe.encrypted	Property used by the application to determine if property files are encrypted. This value is set to `true` if the file is encrypted.
	mxe.LDAPUserMgmt	Indicates whether LDAP owns user management when mxe.userAppServerSecurity = 1. The default value is `1`.
Maximo Asset Management specific Properties	CCMDB.InstallLocation	Product install location. For example, `C:\\IBM\\SMP`.

Table 19. Installation properties (continued)

Category	Property	Definition
	CCMDB.JREInstallLocation	JRE install location. For example, `C:\\IBM\\SMP\\JRE`.
	CCMDB.SDKInstallLocation	SDK install location. For example, `C:\\IBM\\SMP\\SDK`.
	CCMDB.PMP	Unused property.
	CCMDB.Locale	The locale setting of the administrative workstation system. For example, `en`.
	CCMDB.BaseLanguage	Base language that was set for the product. For example, `en`.
	CCMDB.AdditionalLanguages	Additional languages installed for the product.
	CCMDB.DeploySampleData	Binary value that determines whether sample data is to be loaded during the installation. For example, `false`.
	CCMDB.UserShortcuts	Location of the menu for process solution installer and the product console shortcuts.
	CCMDB.InstallType	Type of installation, which includes fix pack, upgrade, or new installation. For example, `Install`.
	CCMDB.DeployEar	Binary value that indicates if EAR files are deployed during the installation. For example, `true`.
process automation engine specific properties	BASE.DeployOptionalContent	Binary value that indicates if optional content is deployed during the installation. For example, `true`.
	BASE.DeployOptionalContentSet	Indicates whether you selected to deploy optional content during the initial upgrade. This value, once set, is a fixed value and cannot be changed. This value will be used for all future upgrades and fix packs.
	BASE.VersionUpgradingFrom	The previous version of process automation engine that was installed.
WebSphere Application Server Network Deployment Thin Client specific Properties	WAS.ThinClientInstallLocation	WebSphere Application Server Network Deployment thin client install location. For example, `C:\\IBM\\SMP\\WASClient`.
	WAS.SOAPConnectorPort	SOAP port of the WebSphere Application Server Network Deployment deployment manager. For example, `8879`.

Table 19. Installation properties (continued)

Category	Property	Definition
	WAS.ThinClientFullyAutomatedConfig	Binary value that indicates if the installation program downloaded the keystore from the WebSphere Application Server Network Deployment deployment manager. If this value is set to `false`, the user has to copy it manually.
	WAS.ThinClientLocalKeystore	Location of the keystore file. For example, `C:\\ibm\\WebSphere\\AppServer\\profiles\\ctgDmgr02\\etc\\trust.p12`.
	WAS.Scripts.Location	Location of scripts used by the installation program. For example, `C:\\IBM\\SMP`
WebSphere Application Server Network Deployment RMI port	WAS.RMIConnectorPort	RMI port on the WebSphere Application Server Network Deployment deployment manager. This port is used if SOAP is not being used. Needed when using IPV6
WebSphere Application Server Network Deployment specific properties	WAS.AutomateConfig	Binary value that indicates if WebSphere Application Server Network Deployment is automatically configured by the installation program. A value of `false` indicates WebSphere Application Server Network Deployment was manually configured before running the installation program.
	WAS.InstallLocation	Installation location for WebSphere Application Server Network Deployment. For example, `C:\\IBM\\WebSphere\\AppServer`
	WAS.DeploymentManagerHostName	Host name of the WebSphere Application Server Network Deployment deployment manager.
	WAS.CellName	WebSphere Application Server Network Deployment CELL name. For example, `ctgCell01`.
	WAS.DeploymentManagerProfileName	WebSphere Application Server Network Deployment profile name. For example, `ctgDmgr01`
	WAS.DeploymentManagerProfileRoot	Location of the WebSphere Application Server Network Deployment profile. For example, `C:/IBM/WebSphere/AppServer/profiles/ctgDmgr01`

Table 19. Installation properties (continued)

Category	Property	Definition
	WAS.ServerProfileName	WebSphere Application Server Network Deployment application server profile name. For example, ctgAppSrv01
	WAS.NodeName	WebSphere Application Server Network Deployment node name. For example, ctgNode01
	WAS.ApplicationServerName	WebSphere Application Server Network Deployment application server name. For example, MXServer
	WAS.ClusterName	WebSphere Application Server Network Deployment cluster name. For example, MAXIMOCLUSTER. This property is designated for future use.
	WAS.AdminUserName	WebSphere Application Server Network Deployment administrator name. For example, wasadmin
	WAS.AdminPassword	WebSphere Application Server Network Deployment administrator password.
	WAS.RemoteAccessUserName	WebSphere Application Server Network Deployment deployment manager system user ID used for tasks such as copying ISC WAR files and fetching the keystore.
	WAS.RemoteAccessPassword	WebSphere Application Server Network Deployment deployment manager system user password.
	WAS.VirtualHost	Name of the WebSphere Application Server Network Deployment virtual host. For example, maximo_host.
	WAS.VirtualHostPort	Port for virtual host for listening for HTTP server. For example, 80.
	WAS.WebServerHostName	Host name where the HTTP server is located.
	WAS.AppServerJvmHeapMin	Minimum heap size setting for the application server JVM. For example, 512.
	WAS.AppServerJvmHeapMax	Maximum heap size setting for the application server JVM. For example, 1024.
	WAS.SibName	Name of the service integration bus. For example, intjmsbus.

Table 19. Installation properties (continued)

Category	Property	Definition
	WAS.SibHiMsg	Service integration bus high message count. For example, `500000`.
	WAS.WebServerName	Name of the WebSphere Application Server Network Deployment web server. Used to manage HTTP server from within WebSphere Application Server Network Deployment. For example, `webserver1`.
	WAS.SibPersistMessages	Binary value that indicates if service integration bus messages are persisted in either the product database or a local derby database. A value of `true` indicates that the messages are persisted.
	WAS.SibDSName	Service integration bus data source name created to access the service integration bus persistence store. For example, `intjmsds`.
	WAS.SibDBType	Database type where the service integration bus messages are being stored. For example, `DB2`.
	WAS.SibDBName	Name of the service integration bus messages database.
	WAS.SibDBInstance	Instance name of the service integration bus database.
	WAS.SibDBServerName	Server name of the system hosting the service integration bus message database.
	WAS.SibDBServerPort	Database server port for the database containing the service integration bus messages. For example, `50005`.
	WAS.SibDBUserName	User ID used to access the persistence data store database for service integration bus messages.
	WAS.SibDBUserPass	Password for user ID named in WAS.SibDBUserName.
	WAS.SibDBInstallDir	Where the service integration bus database is installed. For example, `C:\Program Files\IBM\SQLLIB`.
	WAS.SibDbFencedUser	Fenced user ID for the service integration bus database. This property is only used for databases hosted on UNIX systems. For example, `db2fenc1`.
	WAS.SibDbInstanceAdminUser	Instance owner for the service integration bus database.

Table 19. Installation properties (continued)

Category	Property	Definition
	WAS.SibDbInstanceAdminPassword	Password for the instance owner of the service integration bus database.
	WAS.SibDbRemoteAccessUser	Database server system user used to configure the service integration bus remotely.
	WAS.SibDbRemoteAccessPassword	Password for user ID named in WAS.SibDbRemoteAccessUser.
	WAS.UseDefaultVmmSchema	Unused property.
	WAS.VmmFullyAutomatedConfig	Binary value that indicates if the installation program creates users and directories. For example, `true`.
	WAS.VmmUserRDN	LDAP tree where users are stored. For example, `ou=users,ou=SWG,o=IBM, c=US`.
	WAS.VmmGroupRDN	LDAP tree where groups are stored. For example, `ou=groups,ou=SWG,o=IBM, c=US`.
LDAP Server-specific Properties	LDAP.AutomateConfig	Binary value that indicates whether the installation program automatically configures the directory server. For example, `true`.
	LDAP.Vendor	The type of LDAP repository.
	LDAP.ServerHostName	Host name of the LDAP system host.
	LDAP.AdminDN	Administrator distinguished name. For example, `cn=root`.
	LDAP.AdminPassword	Password for user ID named in LDAP.AdminDN.
	LDAP.ServerPort	Port listening for connection requests. For example, `389`.
	LDAP.InstallLocation	Install location of the directory server. For example, `C:\Program Files\IBM\LDAP\V6.2`.
Database-specific Properties	Database.AutomateConfig	Binary value that indicates whether the installation program automatically configures the database. For example, `true`.
	Database.Vendor	Database type.
	Database.RemoteAccessUserName	Database server system user ID that is used for configure the database remotely.
	Database.RemoteAccessPassword	Password for user ID named in Database.RemoteAccessUserName.

Table 19. Installation properties (continued)

Category	Property	Definition
	mxe.db.driver	Java class name of the JDBC driver. For example, `oracle.jdbc.OracleDriver`. For example `com.inet.tds.TdsDriver`.
	mxe.db.url	JDBC URL of the database. For example, `jdbc: oracle:thin:@`*`mymachine`*`.`*`mydomain`*`.com: 1521:ctginst1`
	mxe.db.initialConnections	Number of database connections to create when the application server is started. For example, 8.
	mxe.db.maxFreeConnections	Maximum number of free database connections available in the connection pool. For example, 8.
	mxe.db.minFreeConnections	Minimum number of free database connections needed in the connection pool in order for more connections to be allocated. For example, 5.
	mxe.db.newConnectionCount	Number of new connections to be created when the minimum free connections are available in the connection pool. For example, 3.
	mxe.db.transaction_isolation	The system install sets the value to: TRANSACTION_READ_COMMITTED. This value cannot be modified.
	mxe.db.format.upper	This value defines the database uppercase function for the system. This value cannot be modified.
	mxe.db.autocommit	This value sets the autocommit mode used for the Write connections. Can be either true or false. The default is `false`. This value cannot be modified.
	mxe.db.systemdateformat	System date format. For Oracle, the value is `sysdate`, and the default value cannot be edited.
	mxe.db.format.nullvalue	The database-specific format of the null value function. The value for Oracle is `NVL`, and the default value cannot be edited.

Table 19. Installation properties (continued)

Category	Property	Definition
	mxe.db.logSQLTimeLimit	The system logs the SQL statements that take longer than the specified time limit. The time is measured in milliseconds (thousandths of a second). The default value is 1000 milliseconds. To disable, edit the file to read: `mxe.db.logSQLTimeLimit=0.`
	mxe.db.fetchResultLogLimit	When this setting is enabled, a stack trace is printed in the log for every business object set that fetches beyond the set limit of rows. The stack trace log is also repeated for every multiple of such fetches. The default is 200 rows. To disable, edit the file to read: `mxe.db.fetchResultLogLimit=0`.
Oracle Properties	Database.Oracle.InstanceName	Oracle instance name.
	Database.Oracle.SoftwareOwner	Owner of the software installation. For example, `oracle`.
	Database.Oracle.SoftwareOwnerPassword	Password for the user ID listed in Database.Oracle.SoftwareOwner.
	Database.Oracle.InstallLocation	Oracle installation location. `For example, /opt/app/oracle/product/10.2.0/db_1.`
	Database.Oracle.DataTablespaceName	Oracle table space name for the product database. For example, `maxdata`.
	Database.Oracle.InstanceLocation	Oracle instance location. For example, `/opt/app/oracle/product/10.2.0/db_1`.
	Database.Oracle.DataTablespaceLocation	Location of Oracle database table space.
	Database.Oracle.DataTablespaceSize	Tablespace size, measured in Mb. For example, `1000`.
	Database.Oracle.DataTablespaceMaxSize	Maximum size of the table space, measured in Mb. For example, `8000`.
	Database.Oracle.TempTablespaceName	Temporary table space name. For example, `maxtemp`.
	Database.Oracle.TempTablespaceLocation	Location of temporary table space.
	Database.Oracle.TempTablespaceSize	Temporary table space size, measured in Mb. For example, `1000`.

Table 19. Installation properties (continued)

Category	Property	Definition
	Database.Oracle.TempTablespaceMaxSize	Maximum size of the temporary table space, measured in Mb. For example, `8000`.
	Database.Oracle.IndexTablespaceName	Index table space name. For example, `maxdata`.
	Database.Oracle.IndexTablespaceLocation	Location of index table space.
	Database.Oracle.IndexTablespaceSize	Index table space size, measured in Mb. For example, `1000`.
	Database.Oracle.IndexTablespaceMaxSize	Maximum size of the index table space, measured in Mb. For example, `8000`.
	mxe.db.schemaowner	Owner of the database schema.
	Database.Oracle.SchemaPassword	Password for user listed in mxe.db.schemaowner.
	Database.Oracle.ServerHostName	Host name of the Oracle server.
	Database.Oracle.ServerPort	Port number used by Oracle. For example, `1521`.
	Database.DBAUserName	Oracle DBA user name. For example, `sys`.
	Database.DBAPassword	Password for user ID listed for Database.DBAUserName.
ADE (DE) Properties	DE.InstalllLocation	Location of the deployment engine.
Application Server Type Properties	ApplicationServer.Vendor	Indicates which application server was chosen during installation. For example, `WebSphere`.

Updating environment data

When you install a second product on the same administrative workstation, or upgrade a single product, the installation program uses values recorded from the previous deployment. These values are stored on the administrative system in the `install.properties` and `maximo.properties` files, and also in the database. If you made any environmental changes to any of the systems used for the original deployment, they must be recorded in the `install.properties` and `maximo.properties` files. They also must be updated in the database. Typically, these types of changes include changing a host name or updating a password.

Before you begin

During a follow-up installation task, the installation program uses values found in the `install.properties` and `maximo.properties` files to complete the upgrade or installation of an additional product. Pending successful use of these credentials, you are not prompted to provide them again. If the installation program fails to log on to the system with the credentials from the properties files, you are prompted to supply current credentials. These values are then written to the appropriate property file.

This method of updating credential information in property files has one exception. Database connection and credential information must always be current before you attempt an upgrade operation. Information for the database connection and credentials are stored in the `maximo.properties` file. Any changes to this information from the time of the original deployment must be recorded manually in the `maximo.properties` file before you upgrade.

Passwords are encrypted within properties files. Update the encrypted values in the properties files with clear text values and then re-encrypt the property file.

About this task

Updates to properties files can be performed by manually editing the appropriate value in a property file. There is a reconfiguration tool available from the Integrated Service Management Library that can be used to update properties. See the Integrated Service Management Library (https://www.ibm.com/software/brandcatalog/ismlibrary/) and search for *IBM Maximo Reconfiguration Tool for Administrative Workstations*.

Procedure

1. Update the property value in the database by using the System Properties application in Maximo Asset Management.
2. Update the database properties in the `maximo.properties` file:
   a. As a precaution, create a backup of the `c:\ibm\smp\maximo\applications\maximo\properties\maximo.properties` file.
   b. Delete the `c:\ibm\smp\maximo\applications\maximo\properties\maximo.properties` file.
   c. Copy `c:\ibm\smp\etc\maximo.properties_orig` to `c:\ibm\smp\maximo\applications\maximo\properties\maximo.properties`
   d. Rename `c:\ibm\smp\maximo\applications\maximo\properties\maximo.properties_orig` to `c:\ibm\smp\maximo\applications\maximo\properties\maximo.properties`.
   e. Edit `c:\ibm\smp\maximo\applications\maximo\properties\maximo.properties` and update the credential or connection information for the target database server.
   f. Encrypt the file `c:\ibm\smp\maximo\tools\maximo\encryptproperties.bat` file.
3. Update the `c:\ibm\smp\etc\install.properties` file on the administrative workstation with any properties that changed. Do not change encrypted password properties. Encrypted password properties are prefixed by `[enc]` in the `installation.properties` file. Passwords can be updated during the next upgrade. If you must update the host name for the IBM WebSphere Application Server Network Deployment server, complete the steps in step 4.
4. Optional: Update the host name for the WebSphere Application Server Network Deployment server.
   a. Copy the keystore file from the WebSphere Application Server Network Deployment deployment manager host to the `c:\ibm\smp\wasclient\etc` directory of the administrative system. The keystore file can be found in `*WAS_HOME*/profiles/ctgDmgr01/etc/trust.p12`.

b. Update the **WAS.DeploymentManagerHostName** property in the `install.properties` file of the administrative system in the target environment.

c. Edit the `C:\ibm\smp\wasclient\thinwasadmin.bat` file and update the following line with the host name of the WebSphere Application Server Network Deployment server:

   ```
   set wsadminHost=-Dcom.ibm.ws.scripting.host=fully_qualified_host_name
   ```

d. Run `C:\ibm\smp\wasclient\thinwasadmin.bat`:

   ```
   thinwsadmin.bat -domain manager user name -password
   ```

Results

After completing these updates, you can upgrade, install a fix pack, or install another product with the corrected values.

Chapter 15. Troubleshooting

If errors occur while you are using the product or middleware installation programs, review the troubleshooting information for solutions to common problems.

When you have corrected all errors, you can reattempt the installation.

Error when starting the middleware installation program

A common cause of middleware installation program errors is running the 32-bit middleware installer on a 64-bit system or running the 64-bit middleware installer on a 32-bit system.

About this task

If you encounter the following error, it indicates that you are attempting to use the 32-bit middleware installation program (`mwi.exe`) on a 64-bit Windows system:

```
CTGIN9051E: The installer or the JRE is not supported on this platform.
```

If you encounter the following error, it indicates that you are attempting to use the 64-bit middleware installation program (`mwi-AMD64.exe`) on a 32-bit Windows system.

```
CreateProcess failed ==> The image file %1 is valid, but for a machine type
other than the current machine
```

Check whether the system you are using to run the middleware installation program is a 32-bit or a 64-bit system, and then run the correct middleware installation program for the system:

32-bit Windows systems
Run `mwi.exe`.

64-bit Windows systems
Run `mwi-AMD64.exe`.

Troubleshooting the middleware installer

You must resolve all errors that occur when you run the middleware installation program for the middleware to be installed correctly.

For more troubleshooting information about a specific middleware component, refer to the documentation for that product.

Middleware installation program troubleshooting feature

The middleware installation program includes a feature that directs you to troubleshooting information when you encounter an error.

When an error occurs during the middleware plan deployment, the middleware installation program displays an error summary panel. The summary panel provides details about the nature of the error and when it occurred. Links that lead you to more detailed information about the error are available when you click **Logs** or **Troubleshooting**.

The **Logs** button opens the directory where the error log files are stored. The **Troubleshooting** button opens the relevant troubleshooting information directly from the product support site. Use the information from the support site to diagnose and resolve the error.

The links that bind an error condition to the URL of the product support site are in the `MWITroubleshooting.xml` file. This file is in the middleware installation program workspace. The middleware installation program downloads the latest version of this file when it is started. If it is unable to connect to the product support site to update the file, it uses the local copy of the file.

Segmentation fault

A segmentation fault occurs when the middleware installation program creates an IBM Tivoli Directory Server instance.

About this task

User authentication restrictions can cause a segmentation fault when the middleware installation program creates an IBM Tivoli Directory Server instance. Non-local user authentication is not permitted during creation of IBM Tivoli Directory Server instances, causing the following error:

```
/opt/ibm/ldap/V6.3/sbin/idscfgdb: line 30: integer: command not found
/opt/ibm/ldap/V6.3/sbin/idscfgdb: line 1098: 29830 Segmentation fault
 ${IDS_LDAP_PRE} ${IDS_LDAP_HOME}/${ITDS_INST_BIN}/${ITDS_BIN}/$PROGNAME "$@"
```

To resolve this issue, complete the following steps:

Procedure

1. Start the middleware installation program, select **Undeploy the Plan**, and then select the option for a **Complete Uninstall**.
2. After the uninstall, exit the installer and delete all DB2 and IBM Tivoli Directory Server instance users and their home directories.
   - db2inst1
   - db2fenc1
   - dasusr1
   - ctginst1
   - idsldap
   - idsccmdb
3. Verify the following conditions:
   - A local user is created to create the IBM Tivoli Directory Server instance. If necessary, update the `/etc/nsswitch.conf` file. The files option must be specified for the **`passwd`** and **`group`** entries. For example:

     ```
     passwd: files
     group: files
     ```
   - NIS must not be configured for the duration of the instance creation process. The `/etc/passwd` file must not have any entries prefixed with a plus (+) sign. NIS can be configured after the instance is created. The `/etc/passwd` file must not have entries prefixed with + (which denotes including NIS user the passwd file configuration
4. Start the middleware installation program and continue with the middleware deployment.

Encountering error CTGIN9048E

During middleware installation using the middleware installer, you might encounter error CTGIN9048E.

About this task

Error CTGIN9048E is encountered when the middleware installation program detects an existing IBM WebSphere Application Server Network Deployment or IBM HTTP Server installation, but cannot find it in the expected directory.

The middleware installation program produces error message CTGIN9048E after the J2EE Server feature has been selected:

```
CTGIN9048E: One or more installations of WebSphere Application Server ND or
IBM HTTP Server were found on your system. The J2EE Server Feature cannot be
selected for deployment while these software installations are on your system.
Remove all of these software installations or unselect the J2EE Server feature.
```

The installation location for the existing IBM WebSphere Application Server Network Deployment or IBM HTTP Server is also reported, but no installation exists in that directory. This error condition can be caused by a previous incomplete installation or uninstallation of IBM WebSphere Application Server Network Deployment or IBM HTTP Server on the system.

Fixing the environment consists of the following steps:

- Clean up the operating system registry.
- Clean up the entries in the `vpd.properties` file.

Procedure

1. Copy and extract the installation image of IBM WebSphere Application Server Network Deployment from the product media to a temporary directory, for example `TEMP`.

   Windows (32–bit)
   `WS-WAS_ND_7.0_Custom_FP15\WAS-ND_WindowsIA32_Custom_v7015.zip`

   Windows (64–bit)
   `WS-WAS_ND_7.0_Custom_FP15\WAS-ND_WindowsIA64_Custom_v7015.zip`

   Linux (64–bit)
   `WS-WAS_ND_7.0_Custom_FP15\WAS-ND_Linux64_Custom_v7015.tar.gz`

   Linux (ppc64)
   `WS-WAS_ND_7.0_Custom_FP15\WAS-ND_LinuxPPC64_Custom_v7015.tar.gz`

   Linux on IBM System z
   `WS-WAS_ND_7.0_Custom_FP15\WAS-ND_Linux390x_Custom_v7015.tar.gz`

   AIX `WS-WAS_ND_7.0_Custom_FP15\WAS-ND_AIXppc64_Custom_v7015.tar.gz`

2. Set the environment.

   ```
   TEMP\WAS\installRegistryUtils\bin\setInstallRegistryUtilsEnv.[bat|sh]
   ```

3. List registry entries.

   ```
   TEMP\WAS\installRegistryUtils\bin\installRegistryUtils.[bat|sh] -listProducts
   ```

   A report is generated from the registry.

   ```
   WNIF0100I: Copyright (c) IBM Corporation 2006; All rights reserved.
   WNIF0102I: Install registry reporter version 1.11

   ---------------------------------------------------------------------
   ```

```
IBM WebSphere Application Server Install Registry Report
----------------------------------------------------------------------------

Report at date and time February 4, 2011 4:19:11 AM EST

----------------------------------------------------------------------------

Product Installed
----------------------------------------------------------------------------
Offering ID                  ND
Installation Location        C:\Program Files\IBM\WebSphere\AppServer
Version                      6.1.0.29

Product Installed
----------------------------------------------------------------------------
Offering ID                  UPDI
Installation Location        C:\Program Files\IBM\WebSphere\UpdateInstaller
Version                      7.0.0.5

Product Installed
----------------------------------------------------------------------------
Offering ID                  IHS
Installation Location        C:\Program Files\IBM\HTTPServer
Version                      6.1.0.29

Product Installed
----------------------------------------------------------------------------
Offering ID                  PLG
Installation Location        C:\Program Files\IBM\HTTPServer\Plugins
Version                      6.1.0.29

----------------------------------------------------------------------------
End Install Registry Report
----------------------------------------------------------------------------
```

4. Check for IBM WebSphere Application Server Network Deployment related entries. If any IBM WebSphere Application Server Network Deployment entries are listed, you must clean the registry entry using the **installRegistryUtils** command.

   ```
   TEMP\WAS\installRegistryUtils\bin\installRegistryUtils.[bat|sh] -cleanAll
   ```

5. Edit the vpd.properties file. Remove any entries related to IBM WebSphere Application Server Network Deployment version 6 or version 7, and then save the file. IBM WebSphere Application Server Network Deployment-related entries are prefixed with WSBAA70, WSBAA61, WSIHS70, WSIHS61, WSPAA70 and WSPAA61. The vpd.properties is found in the following directories:

   Windows

   C:\WINNT or C:\windows

   AIX and Linux

   /usr/lib/objrepos/

6. Rerun the middleware installation program.

Encountering error CTGIN9042E

During middleware installation using the middleware installer, you might encounter error CTGIN9042E which occurs during the installation step for WebSphere Application Server Network Deployment.

About this task

If you encounter error CTGIN9042E through the normal use of the middleware installation program, it might be related to stale entries in the CEI registry.

In order to troubleshoot this error, complete the following steps:

Procedure

1. First check `de_processreq.log` for failures related to **`VerifyLogsInInstallLogs`** Action. The `de_processreq.log` file can be found at:

   ```
   <workspace>\<machine name>\deploymentPlan\MachinePlan_<machine shortname>
   \00009_WAS_ND_6.1\install\01_BASE/[INSTALL_<processing.req.id>]/logs/
   de_processreq.log
   ```

   So, for example, if the workspace is at `C:\ibm\tivoli\workspace`, the machine name is **`mymachine`**, and the **`processing.req.id`** is created as a **`date_timestamp`**, then the `de_processreq.log` would be in:

   ```
   C:\ibm\tivoli\mwi\workspace\mymachine.ibm.com\deploymentPlan\
   MachinePlan_mymachine\00009_WAS_ND_6.1\install\01_BASE\
   [INSTALL_1130_06.54]\logs
   ```
2. Next, check for any stale WebSphere Application Server Network Deployment entries:
   1. Extract the native image of WebSphere Application Server Network Deployment:

      Windows
      WAS-ND_WindowsIA32_Custom_v61023

      Linux WAS-ND_LinuxIA32_Custom_v61023.tar.gz

      AIX WAS-ND_AIXppc64_Custom_v61023.tar.gz
   2. Open the console window.
   3. Browse to the bin folder of extracted image. For example:

      ```
      \WAS\installRegistryUtils\bin
      ```
   4. List registry entries:

      Windows
      `installRegistryUtils.bat -listProducts`

      UNIX **`installRegistryUtils.sh -listProducts`**
   5. Check for WebSphere Application Server Network Deployment related entries. If any WebSphere Application Server Network Deployment entries are listed, even if you have successfully uninstalled WebSphere Application Server Network Deployment, you must clean the registry entry.
3. Clean the registry entries:
   1. Clean WebSphere Application Server Network Deployment entries from the registry:

      ```
      installRegistryUtils -cleanProduct -offeringID ND -installLocation
      <WAS installation location path>
      ```
   2. Edit the `vpd.properties` file, remove any WebSphere Application Server Network Deployment entries, and then save the file. The file is in the installation directory of the operating system:

      Windows
      `C:\WINNT` directory or `C:\windows` directory

      UNIX `/usr/lib/objrepos/`
4. After cleaning the registry, run the middleware installation program again and Restart the plan. WebSphere Application Server Network Deployment is now successfully installed in the default location, for example, `C:\Program Files\IBM\WebSphere\AppServer` for Windows.

Encountering error ACUINI0044E

During middleware installation using the middleware installer, you might encounter error ACUINI0044E which occurs during the install step for the deployment engine.

About this task

If you encounter error ACUINI0044E through the normal use of the middleware installation program, it might be related to a failure of the deployment engine to be installed or started. The following messages will be displayed after a failure to deploy the deployment engine is encountered:

```
Deployment Engine did not start successfully. Please try to manually
start the Deployment Engine and restart the installer.

ACUINI0044E Failed to register and start Deployment Engine
IBM ADE Service
```

In order to troubleshoot this error, complete the following steps:

Procedure

1. Exit the middleware installation program.
2. Restart the deployment engine.
   - For Windows, use the following command:
     ```
     net start "IBM ADE Service"
     ```
   - For UNIX, use the following command:
     ```
     /usr/ibm/common/acsi/bin/acsisrv.sh -start
     ```

   If the deployment engine is started successfully, restart the middleware installation program and resume middleware deployment. If the deployment engine fails to start, you have to manually uninstall the deployment engine. This action also eliminates the deployment engine registry information for other products installed on the system, so use caution when uninstalling the deployment engine.

“Common deployment failures” on page 203
General troubleshooting techniques can be used to determine common deployment failures.

Improper configuration of DB2 or IBM Tivoli Directory Server

While running the middleware installation program on an AIX system, you encounter the error message CTGIN9042E, which relates to a failure to properly configure DB2 or IBM Tivoli Directory Server.

If you encounter error CTGIN9042E through the normal use of the middleware installation program on an AIX machine, check the following log files to determine the precise cause of the error:

Check the `mwi.log` file located within the workspace directory (for example:`/ibm/tivoli/mwi/workspace`), and look for an error like the following sample:

```
Caused by:
<workspace>/<machine name>/deploymentPlan/MachinePlan_<machine name>/
00005_DB2_Configuration/install/02_CONFIG/02_CONFIG_AIX.xml:173: Failed
 to create database instance ctginsxy.
```

Also check the createinstance.log file at <workspace>/<machine name>/deploymentPlan/MachinePlan_<machine shortname>/ 00005_DB2_Configuration/install/02_CONFIG/[INSTALL_<processing.req.id>]/ logs/createinstance.log

for an error like the following sample:

```
Caused by: <workspace>/<machine name>/deploymentPlan/MachinePlan_
<machine name>/00008_ITDS_Configuration/install/02_CONFIG/02_CONFIG_AIX.xml:173:
Failed to create itds database instance itdsccmxy.
```

Check the startInstanceTool.log file at <workspace>/<machine name>/deploymentPlan/MachinePlan_<machine shortname>/ 00008_ITDS_Configuration/install/02_CONFIG/[INSTALL_<processing.req.id>]/ logs/startInstanceTool.log

for any error like the following sample:

```
DBI1703E No valid service name or port number found
```

If you locate any of these errors in the log files listed, the error can be attributed to a failure to properly configure either DB2 or IBM Tivoli Directory Server.

To resolve this issue, complete the following steps:

1. Click **Finish** to exit out of the middleware installation program install wizard.
2. Restart the middleware installation program and proceed through the wizard until you reach the Restart or Undeploy the Plan panel.
3. Select **Undeploy the Plan**, and then click **Next**.
4. Select **Partial uninstall**, and then click **Next**.
5. Select only the **Configuration for DB2 Enterprise Server Edition** option, and then click **Next**.
6. Proceed through the panels to complete the uninstall and click **Finish** to exit the installer.
7. Download the mwi_db2instance.sh and mwi_itdsinstance.sh files attached to this document to your local system.

   Alternatively, you can create your own copies of these files.

   a. Create a text file named mwi_db2instance.sh and add the following content:

   ```
   #!/bin/ksh
   port1=0
   var1=3
   if [ -f /etc/services ]
    then
   if [ $# -eq 0 ]
    then
   cat >> /etc/services << EOF
   DB2_ctginst1  60000/tcp
   DB2_ctginst1_END 60003/tcp
   EOF
   elif [ $# -gt 0 ]
    then
   port1=`expr $2 + $var1`
   cat >> /etc/services << EOF
   DB2_$1 $2/tcp
   DB2_$1_END $port1/tcp
   EOF
   fi
   fi
   ```

b. Create a text file named mwi_itdsinstance.sh and add the following content:

```
#!/bin/ksh
port1=0
var1=3
if [ -f /etc/services ]
 then
if [ $# -eq 0 ]
 then
cat >> /etc/services << EOF
DB2_idsccmdb 60004/tcp
DB2_idsccmdb_END 60007/tcp
EOF
elif [ $# -gt 0 ]
 then
port1=`expr $2 + $var1`
cat >> /etc/services << EOF
DB2_$1 $2/tcp
DB2_$1_END $port1/tcp
EOF
fi
fi
```

8. Based on the deployment choices you made in the middleware installation program, run the following scripts:
   - If you elected to deploy both the Database Server and Directory Server, run both the mwi_db2instance.sh and mwi_itdsinstance.sh scripts.
   - If you elected to deploy the Database Server only, run the mwi_db2instance.sh script.
   - If you elected to deploy the Directory Server only, run the mwi_itdsinstance.sh script.
9. Run the middleware installation program again and select the option to **Restart the plan**, which installs everything you selected in the original deployment plan.
10. Proceed through the rest of the installation process and exit the installation program when complete.

When using the mwi_db2instance.sh script, DB2 is installed with default values if you initiate the script without passing any parameters. If you want to use custom values run mwi_db2instance.sh and pass values for DB2 instance name and the DB2 port number in the following order:./mwi_db2instance.sh ctginsxy 50007 where ctginzxy and 50007 are the values entered in middleware installation program DB2 Configuration Panel.

When using the mwi_itdsinstance.sh script, IBM Tivoli Directory Server is installed with default values if you initiate the script without passing any parameters. If you want to use custom values run mwi_itdsinstance.sh and pass values for the instance name and the port number in the following order: ./mwi_itdsinstance.sh itdsccmxy 60007 where itdsccmxy and 60007 are the values entered in middleware installation program IBM Tivoli Directory Server DB2 instance Configuration Panel.

Incorrect idsccmdb user password

If you encounter error CTGIN9042E through the normal use of the middleware installation program, it might be related to the fact that there is an existing user named idsccmdb on the system, but with a different password than the one entered in the middleware installation program.

The error might look like the following sample:

```
CTGIN9042E: Errors were encountered during the execution of the step
Configuration for IBM Tivoli Directory Server
```

Check the configureDB.log file for an error like the following sample:

```
GLPCDB018E The DB2 administrator ID or password you specified is not valid.
```

This message indicates that the existing IBM Tivoli Directory Server user idsccmdb has different password in the system.

The configureDB.log file is located at: <Workspace>\<machine name>\deploymentPlan\MachinePlan_<machine shortname>\00008_ITDS_Configuration\install\02_CONFIG\logs\configureDB.log

Windows
So, for example in Windows, if the workspace is located at: C:\ibm\tivoli\workspace, the machine name is mymachine, then the configureDB.log file would be located in: C:\ibm\tivoli\mwi\workspace\mymachine.ibm.com\deploymentPlan\MachinePlan_mymachine\00008_ITDS_Configuration\install\02_CONFIG\logs

Linux
In Linux, if the workspace is located at: /root/ibm/tivoli/mwi/workspace, the machine name is mymachine, then the configureDB.log would be located in: /root/ibm/tivoli/mwi/workspace/mymachine.ibm.com/deploymentPlan/MachinePlan_mymachine.ibm.com/00008_ITDS_Configuration/install/02_CONFIG/logs

AIX
In AIX, if the workspace is located at: /ibm/tivoli/mwi/workspace, the machine name is mymachine, then the configureDB.log would be located in: /ibm/tivoli/mwi/workspace/mymachine.ibm.com/deploymentPlan/MachinePlan_mymachine.ibm.com/00008_ITDS_Configuration/install/02_CONFIG/logs

To resolve this issue, complete the following steps:

1. If you have not done so, click **Finish** to exit out of the middleware installation program install wizard.
2. Resolve the issue using one of the following methods:
   - If you are the Administrator for that machine and if you know the password for the user idsccmdb you can use the same password for the middleware installation program installation.
   - You can delete the user idsccmdb and restart the middleware installation program.
   - You can set or change the password for existing IBM Tivoli Directory Server user idsccmdb.

     To set the password complete the following steps

     Windows

     a. Right-click on My Computer icon and click **Manage** menu item.
     b. From the Computer Management console, select Local Users and Groups in System Tools.
     c. Expand Local Users and Groups and then select Users
     d. Right-click on the idsccmdb user and then click the set password menu item.
     e. Enter the password, confirm it, and then click **OK**
     f. Click **OK** once again.

Linux AND AIX

a. Log in as root and open command prompt.
b. Run the following command at terminal:

```
# passwd idsccmdb
```

c. Enter the new password and confirm it.

3. Navigate to the directory containing the middleware installation program image and restart the middleware installation program.
4. Select **Undeploy the Plan** and click **Next**.
5. Select **Partial Uninstall** and click **Next**.
6. Select **Configuration for IBM Tivoli Directory Server** and click **Next**.
7. Click **Undeploy** to start the uninstall.
8. After install completes click **Finish** to exit the wizard.
9. Navigate to the directory containing the middleware installation program image and restart the middleware installation program.
10. Select **Restart the Plan** and click **Next**.
11. Specify the directory for the middleware install images and click **Next**.
12. Specify the temporary directory and click **Next**.
13. After disk space checks are completed, click **Deploy** to start the install.
14. After install completes click **Finish** to exit the wizard.

Incorrect service pack requirement for AIX

When running the middleware installation program on AIX platforms, you might encounter the following message: `CTGIN9061E: Unsupported Technology Level. OS Technology Level should be 06 or greater and SP level 02 or greater.`

This message is shown when the cited service pack level is incorrect. While the error message indicates SP level 02 or greater is a prerequisite, SP level 01 or greater is the actual middleware installation program prerequisite.

Failure when system directories cannot be renamed

During middleware installation you encounter CTGIN9042E during the execution of a number of installation steps. This error can occur during the execution of any of the middleware steps where renaming of the product install directories has failed.

If you encounter the following error message: `CTGIN9042E: Errors were encountered during the execution of step <step_name>`, where <step_name> can be any of a number of middleware installation steps.

This renaming of existing directories can fail in certain situations. For example:

1. If it has been previously created as a file system (instead of a directory within a defined file system).
2. If the file system or directory has been created with Read Only access.

To determine if this situation is the cause of the error complete the following steps:

1. Check the `DeploymentPlan.log`

   This log file is located at `/ibm/tivoli/mwi/workspace/<Machine_name>/deploymentPlan/logs/[INSTALL_`*`<date_time_stamp>`*`]/DeploymentPlan.log`, where `/ibm/tivoli/mwi/workspace` is the default middleware workspace or the path you specified on the installer workspace panel, and <*Machine_name*> is the host name of the machine on which you are installing.

Locate the step name that has failed.

Also check the DeploymentPlan.log for the following sample error text:

```
ml:284: The following error occurred while executing this line:
/ibm/tivoli/mwi/workspace/<host name>/deploymentPlan/MachinePlan_<host name>
/deploymentPlan/MachinePlan_00004_<middleware>/common/Utils.x

ml:544: Deployment Engine command de_processReq reported an error.
```

Check the de_processReq output file at /ibm/tivoli/mwi/works pace/<host name>/deploymentPlan/MachinePlan_<host name>/00004_<middleware>/install/01_BASE/[INSTALL_1215_04.00]/logs/de_processreq.log_utf8

Check de_trace.log at /ibm/tivoli/mwi/workspace/<host name>/deploymentPlan/MachinePlan_<host name>/00004_<middleware>/install/01_BASE/[INSTALL_1215_04.00]/logs.

2. Check the location and the logs indicated by the error message from step #1:

   Check de_processreq.log_utf8 at /ibm/tivoli/mwi/workspace/<host name>/deploymentPlan/MachinePlan_<host name>/00004_<middleware>/install/01_BASE/[INSTALL_1215_04.00]/logs/de_processreq.log_utf8 for the following error text:

   ```
   <errorMessage>[com.ibm.ac.si.ap.action.ExternalCommandActionException:
   ACUOSI0050E External command action failed with return code 1.
   <actionErrorEvent actionID=RenameExistingInstallLocation_Unix
   actionName="externalCommand">ACUCME1100E</actionErrorEvent>
   ```

   If this error is found in de_processreq.log_utf8, check for the existence of the following error file that might contain additional information: <Product_Name>_RenameExistingInstallLocation_Unix_<Date_Time_stamp>.err

IBM Tivoli Directory Server starts in configuration mode

IBM Tivoli Directory Server version 6.3, which is installed by the middleware installer, starts in configuration mode when it is installed with DB2 version 9.7.

About this task

IBM Tivoli Directory Server version 6.3, which is installed by the middleware installer, starts in configuration mode when it is installed with DB2 version 9.7. This issue occurs when you install IBM Tivoli Directory Server version 6.3 with DB2 version 9.7 on Microsoft Windows Server 2008 systems. IBM Tivoli Directory Server version 6.3 starts correctly when it is installed with DB2 version 9.7, fix pack 2.

Procedure

1. To start IBM Tivoli Directory Server version 6.3 in normal mode, you run a startup script that is provided with the middleware installation program. In the MWI directory of the installation image or on the product media, start the startITDS.bat file.
2. Specify the following values as the command-line parameters when you run the script: startITDS.bat -l *ITDS-Home* -I *instance-name* -p *Port No* -s *secure-port*

Option	Description
ITDS-Home	The directory where IBM Tivoli Directory Server is installed in the system. By default, the value "C:\Program Files\IBM\ldap\V6.3" is used.
instance-name	The database instance name that is used by IBM Tivoli Directory Server. By default, the value idsccmdb is used.
Port No	The TCP port that is used by IBM Tivoli Directory Server. By default, port 389 is used.
secure-port	The TCP secure port that is used by IBM Tivoli Directory Server. By default, port 636 is used.

Alternatively, you can use a text editor to modify the default values that are used by the script.

3. The script opens a new console window to start IBM Tivoli Directory Server. Do not close the console window.

Middleware setup script error codes

Errors that occur when you run the middleware setup scripts are categorized by codes. The error codes appear on the screen during installation and they are stored in an error log file.

Table 20. Middleware installation program setup script error codes

Error Code	Error	Description
11	Unsupported operating system	The middleware installation program or one of the middleware products cannot run on this operating system.
12	Unsupported Linux distribution	The middleware installation program or one of the middleware products is not supported on this Linux kernel. Only Red Hat Enterprise Linux and SUSE Linux Enterprise Server are supported.
13	Unsupported kernel bit mode	The middleware installation program is supported on Linux 32-bit or 64-bit mode and on AIX 64 bit mode.
14	Unsupported processor architecture	The middleware installation program or one of the middleware products is not supported on this processor architecture. Only x86 and AMD64 architecture are supported.
21	Env variable mwi_launchpadroot(UNIX) / LaunchPadBatchPath(Win) is not set	The environment variable must be set to the middleware installation program installation files location: **Windows** LaunchPadBatchPath **Linux and UNIX** mwi_launchpadroot
22	The middleware installation program file is not found	The middleware installation program installation file is missing or not accessible. Ensure that the specified file exists in the current directory.
31	Host name is not a fully qualified domain name.	The middleware installation program or one of the middleware products requires a fully qualified host name. Alternatively, you can provide the IP address for the system.

Table 20. Middleware installation program setup script error codes (continued)

Error Code	Error	Description

32	SELinux is enabled or set in Enforcing mode	Middleware product installation fails with the following error:
		`JRE could not be found on the system`
		Disable Security-Enhanced Linux by using one of the following methods:
		• `setenforce 0`
		• Add the following entry to the `/etc/system` file:
		`set fmac_enforcing = 0`

33	The library `libstdc++.so.5` (64-bit) is not installed.	The installer requires the 64-bit version of the `libstdc++.so.5` system library, which is in the`/usr/lib64/libstdc++.so.5` folder. If this library is not installed, you must search for a Resource Package Manager (RPM) package that contains `libstdc++.so.5` (64-bit) and install it.
34	The library `libstdc++.so.5` is not installed.	The installer requires the `libstdc++.so.5` system library, which is in the `/usr/lib/libstdc++.so.5` folder. If this library is not installed, you must search for a Resource Package Manager (RPM) package that contains `libstdc++.so.5` and install it.

Troubleshooting middleware uninstall

Use the information contained in this section to troubleshoot middleware uninstall issues.

Use the information contained in this section to troubleshoot errors encountered uninstalling middleware installed through the middleware installation program.

WebSphere Application Server Network Deployment uninstallation fails after unsuccessful binding to LDAP directory

WebSphere Application Server Network Deployment installation fails when using the middleware installation program. This error occurs when you undeploy the middleware deployment plan. The error is related to an unsuccessful binding to the LDAP directory.

About this task

The middleware installation program configures WebSphere Application Server Network Deployment security. Security is configured using an LDAP directory. The LDAP directory can be hosted by Microsoft Active Directory or IBM Tivoli Directory Server. You need credentials to access the remote LDAP server. The set of credentials includes:

- The host name or IP address
- Port in which LDAP server is running
- LDAP base entry
- User, Group, and Organization suffix
- Bind DN and password

WebSphere Application Server Network Deployment administrator credentials must exist in the remote LDAP Directory. Middleware installation fails if the wrong credentials are provided. This failure occurs during the WebSphere Application Server Network Deployment configuration step. Once the initial installation failed, the uninstallation (undeployment) of the deployment plan also fails. WebSphere Application Server Network Deployment cannot issue the stopManager command to stop the ctgDmgr01 profile. This condition results in the following error:

```
SECJ0305I: The role-based authorization check failed for admin-authz operation
Server:stop:java.lang.Boolean:java.lang.Integer.  The user UNAUTHENTICATED
(unique ID: unauthenticated) was not granted any of the following required roles:
operator, administrator.
```

If you encounter the error described, complete the following steps as a workaround:

Procedure

1. For UNIX systems, complete the following steps:
   a. List Java processes.
      ```
      ps -ef | grep -i java
      ```
   b. Locate the process-id of the Java thread: `<WebSphere Install Location>/java/bin/java` and then kill the process.
      ```
      kill -9 <process-id>
      ```
   c. Restart the middleware installation program to undeploy the plan.
2. For Windows systems, complete the following steps:
   a. Change the startup type for key services from the Services control panel. Change the startup type from Automatic to Manual.
      ```
      IBM WebSphere Application Server V7.0 - ctgCellManager01
      IBM WebSphere Application Server V7.0 - nodeagent
      ```
   b. Restart the system.
   c. Restart the middleware installation program to undeploy the plan.

Troubleshooting the product installation program

If you experience a failure using the product installation program, you must troubleshoot the issue before continuing.

Begin with general troubleshooting techniques. These techniques help you determine which portion of the installation failed.

General troubleshooting of the product installation program

During product installation, you might need to troubleshoot errors that occur within the installation program.

Because Maximo Asset Management is typically deployed as a distributed system, errors can be generated from multiple sources. The installation error panel displays any failure messages encountered during execution of the configuration step of the deployment. These messages direct you to the source of the problem and the set of logs to examine for further details.

All installation-related messages begin with the prefix CTGIN. Informational message end with a suffix of I, warning messages end with a suffix of W, and error messages end with a suffix of E.

There are four main categories of logs that can be used for installation error remediation.

- Install trace logs

- Solution installation logs
- Maximo logs
- Middleware logs

Install trace logs

Install trace logs are generated on the Maximo Asset Management administrative workstation in the `*install_home*\logs` directory. These logs can be searched for the error message displayed on the installation error panel. They provide more diagnostic information about why the error occurred. Installation trace logs contain historical data about when the installation program was started and which options were chosen for the deployment. It also contains information about updates and fix packs.

Searching on the term maxinst places you in the general proximity of information about database configuration.

If you encounter an error during a validation task, install trace logs can also be located within the `C:\Documents and Settings\Administrator` directory. They are moved to the *install_home*`\logs` directory during execution of the configuration step of the deployment.

The following trace log files are found in the *install_home*`\logs` directory:

CTGInstallTrace00.log

This log contains information produced by the Maximo Asset Management installation program.

The log includes details about:

- Embedded calls to the process solution installation program
- The automated configuration of WebSphere Application Server Network Deployment.

Information generated from subsequent invocations of the Maximo Asset Management installation program or the process solution installation program is appended to this file.

The following **success** message examples are found in the CTGInstallTrace00.log file. These messages can be used to determine which phases of the installation were successful:

- CTGIN2114I: The database was created successfully
- CTGIN2135I: Tablespace maxdata created successfully
- CTGIN2135I: Tablespace maxtemp created successfully
- CTGIN2079I: process automation engine database configuration completed successfully (This message indicates that maxinst finished successfully.)
- CTGIN2222I: WebSphere Application Server creation successful
- CTGIN2188I: Creation and configuration of service integration bus successfully completed
- CTGIN2184I: Creation and configuration of JMS resources successfully completed
- CTGIN2310I: Application server security was successfully enabled for the process automation engine
- CTGIN2253I: buildmaximoear.cmd completed successfully

- CTGIN2224I: Deployment of application MAXIMO was successful
- CTGIN2253I: buildmxiehsear.cmd completed successfully
- CTGIN2224I: Deployment of application MAXIMOIEHS was successful
- CTGIN2208I: runConfigurationStep completed successfully
- CTGIN2370I: The installation finished successfully

The following **warning** message example is found in the CTGInstallTrace00.log file. This message indicates that while a function completed successfully, you need to perform additional steps outside of the installation program.

- CTGIN2420W The undoConfiguration function completed but some manual clean-up is required for the following component: <Variable formatSpec="{0}">manual component</Variable>.

The following **error** message example indicates that while the installation completed, there were some serious errors.

- CTGIN2371E: The installation is finished, but some serious errors occurred during the install.

In this error case, open the CTGInstallTrace00.log file and examine the most recent logged information. Determine what caused the failure. In some cases, the error is the result of a failed configuration task that was attempted by Maximo Asset Management installation program configuration scripts.

CTGInstallMessage00.log
This log contains named message statements generated by the Maximo Asset Management installation program, configuration tasks, and the process solution installation program during the installation.

CCMDB_install.log
This log contains information about the Maximo Asset Management installation program itself, including values that you provided and options you selected during the installation.

In some instances, you find trace logs with 01, 02, and so on, in the file name. These files contain information like what is found in the files that include 00 in the file name. These files are generated when a second JVM is started during the installation, and it begins logging information.

Solution installation logs

Solution installation logs are generated on the Maximo Asset Management administrative workstation in the `*install_home*\solutions\logs` and `C:\program files\ibm\common\acsi\logs\<*administrative user*>` directories. These logs provide in-depth information about exceptions and errors related to process manager packages, other PSI packages, and also the deployment engine.

Maximo logs

Core components of Maximo Asset Management include deployment utilities such as updatedb, configdb, maxinst, tdtoolkit, buildmaximoear, and deployapplication. Logs for these components are generated on the Maximo Asset Management administrative workstation in the *install_home*\maximo\tools\maximo\log directory.

Middleware logs

Native middleware logs for the database server can be examined for failures occurring on the middleware server.

J2EE-related logs generated for the WebSphere Application Server application server, deployment manager, and node agent are used to troubleshoot EAR file deployment failures. If you encounter errors related to EAR file deployment, examine the `SystemOut.log` and `SystemError.log` files.

Log utility

When engaging IBM product support services, be prepared to provide log files in an archive file. The `LogZipper.bat` utility provided in the `<`*`install_home`*`\scripts` directory can be used for this task. If you use the `LogZipper.bat` utility, all relevant log files are archived in *`install_home`*`\debug\`*`YYYYMMDD_hhmmss`*`.zip`.

When you contact IBM support personnel, you are asked to provide log files from the following directories:

- <*WAS_PROFILE_HOME*>\logs (from both the WebSphere Application Server Network Deployment application server and the WebSphere Application Server Network Deployment deployment manager)
- *install_home*\logs
- *install_home*\solution/logs
- *install_home*\maximo\applications\maximo\properties
- *install_home*\etc\install.properties
- <*Middleware_Installer_Workspace*>

IBM Support Assistant Workbench

The IBM Support Assistant (ISA) V4 is a free serviceability workbench that you can download from IBM. ISA, using product-specific add-ons, provides a central location to learn more about products, gather data for troubleshooting problems, and manage problem submissions.

The IBM Service Management and IBM Maximo Asset Management (Maximo Asset Management) add-ons to the ISA Workbench provide a quick and direct way to learn more about the product. If you encounter a problem with Maximo Asset Management, you can use the ISA with these add-ons to search support documents. These documents supply fixes or recommendations and quickly gather relevant logs for diagnosis. You can use the Log Analyzer to view the logs and use the filter feature to reduce the amount of data to examine. The symptom catalogs can be used to analyze the logs.

You can use the ISA to perform these tasks:

- *Search documents concurrently*. Rapidly search IBM documentation in many different locations at the same time for answers to your questions or problems. ISA returns results that are categorized by source for easy review.
- *Access product information*. Quickly access key product information links, such as the product support page and home page, online product documentation. Also access RSS feed information for the latest Flash notes, APARs, fixes, and technotes.

- *Gather data*. Collect files to document problems related to installation, databases, security, and general problems relevant to troubleshooting your environment. The collected data is packaged in compressed form for transmission to IBM.
- *Analyze log data*. Use the Log Analyzer to review collected log files and troubleshoot problems.
- *Report problems*. Connect to the IBM Electronic Service Request system to open and update Problem Management Records. Send the information that the IBM Service Management data collection scripts gather to IBM for diagnosis.

Deployment properties

Deployment of ISM solutions often happens in stages. You might install one ISM product and then deploy another at a later date. Follow-up deployments rely on the installation and configuration data from previous installations. For example, how to connect to the database used with the original product deployment. This information must be persisted and protected. This data is persisted by storing deployment data in both the product database and a set of properties files. This redundancy protects the deployment information in case anything were to happen to the database.

After a successful deployment, deployment properties are kept both in the database and in two property files.

maximo.properties
: The `maximo.properties` file is an encrypted file which is in the *`install_home`*`\maximo\applications\maximo\properties\` directory. This property file contains database connection properties.

install.properties
: The `install.properties` file is an encrypted file which is located in the *`install_home`*`\etc\` directory and contains most properties related to the deployment.

Errors related to an inability to connect or authenticate to middleware servers during an upgrade or fix pack installation might be caused by obsolete property values. For example, if you change the password for you used during the initial Maximo Asset Management installation without updating that value in the relevant property file. The next installation action fetches the outdated value from the property file and a failure occurs.

License files

License files are on the media and are not packaged with the installation program. If you copy the installation program from the product media to the file system, the License directory must also be copied.

Problem resolution

The configuration step of the Maximo Asset Management installation process occurs after you have navigated through all the installation wizard panels and then clicked **Install**.

Errors experienced before the configuration step are typically related to the inability of the installation program to verify that input values you provided. If you experience this error, investigate the trace logs, resolve the issue, and then proceed through the rest of the installation wizard.

If you experience an error after the configuration step, you must exit the installation program. Examine the trace, solution install, and Maximo logs. Resolve the issue and then complete the installation using the taskrunner utility by starting it from the command line:

```
C:\IBM\SMP\scripts\taskRunner.bat CONTINUE STOPONERROR
```

Note: If you reboot the system, you are not be able to use the taskrunner utility to run configuration scripts. Taskrunner data stores are not persisted. If you intend to use the taskrunner utility, do not reboot your system.

The taskrunner utility resumes the installation at the point where the last successfully completed task was recorded in the previous attempt. If you run taskrunner with the **NOSTOPONERROR** parameter, the taskrunner continues despite errors.

“Installation properties” on page 172
Installation properties are recorded in properties files during a deployment and are used as input by future install-related actions. Installation properties are found in the install.properties and maximo.properties files as well as the database. You should only modify properties found in the install.properties file that are related to host names or user IDs. Changing values for other properties can severely impact your ability to perform future installation actions, upgrades and fix pack installations.

➦ http://www.ibm.com/software/support/isa/isa41/install.html

Common deployment failures

General troubleshooting techniques can be used to determine common deployment failures.

Starting the installation program

If you start the product installation program from a drive that is different than the one you choose as the installation destination, the installation fails. This behavior occurs when you are starting the installation program directly or though the product launchpad.

To resolve this problem, start the installer or launchpad application from the drive where you install the product.

For example, if you want to install the product on the g: drive, open a command prompt and switch to the g: drive before invoking the installer. So, if your installer was on the d: drive the command might look like the following:

```
g:\> d:\temp\install.exe
```

(where g:> is your Windows command prompt)

Windows explorer normally sets the system default drive to "%HOMEDRIVE%" which is typically the drive where Windows is installed. If that is the target drive of the product install you can start the installer or launchpad from Windows Explorer.

If you plan to install the product on a drive other than the one hosting Windows, do not start the installer from Windows Explorer. Start the installer from the command line as described earlier.

Remote access configuration

If you choose to configure middleware using the automated configuration feature of the Maximo Asset Management installation program, you must enable a remote access protocol for each system that is hosting a middleware server. Messages with the prefix CTGRI are found in the CTGInstallTrace.log file. They are related the Maximo Asset Management installation program not being able to access remote systems designated as part of the product deployment.

Ports An error reporting a failure to reach the remote host can sometimes be related to a required port not being available to the Maximo Asset Management installation program. Ensure that the following ports are accessible on servers that are hosting middleware:

445 Port 445 is used for SMB over TCP.

139 Port 139 is used for TCP NetBIOS connections.

Remote registry permissions

Error CTGRI0011E is issued if the user ID provided to the installation program that is used to access a remote Windows system does not have appropriate permissions to the registry. Remote access to the registry is determined by the HKLM\System\CurrentControlSet\Control\SecurePipeServers\winreg registry key entry. Visit the Microsoft help and support website for more information. Use the issue search facility to locate the article on how to manage remote access to the registry.

Connection exceptions

Remote access connection exceptions typically manifest themselves as either an authorization failure or as a host connection failure. Search the `CTGInstallTrace.log` file to determine the cause of the connection exception.

An authorization error is triggered by an incorrect user ID or password value supplied to the Maximo Asset Management installation program. Errors for this type of exception typically look like the following example:

```
SEVERE: EXIT ^RxaConnectFailure:^o^{{com.ibm.tivoli.remoteaccess.
RemoteAccessAuthException: CTGRI0000E Could not establish a connection
to the target machine with the authorization credentials that were provided.
 at com.ibm.tivoli.remoteaccess.BaseProtocol.beginSession
  (BaseProtocol.java:522)
 at com.ibm.tivoli.ccmdb.install.common.util.rxa.RxaHost.init
  (RxaHost.java:130)
 at com.ibm.tivoli.ccmdb.install.common.util.rxa.RxaHost.<init>
  (RxaHost.java:78)
 at com.ibm.tivoli.ccmdb.install.common.ia.CmnInstallAnywhereUtils.getOSType
  (CmnInstallAnywhereUtils.java:303)
 at com.ibm.tivoli.ccmdb.install.foundation.appsvr.FndWasRemoteActions.
  install
  (FndWasRemoteActions.java:237)
 at com.zerog.ia.installer.actions.CustomAction.installSelf(DashoA10*..)
 at ZeroGab8.run(DashoA10*..)
```

A host connection failure is triggered when the remote protocols Maximo Asset Management installation program cannot reach the remote system using the protocols it supports. This error typically looks like the following example:

```
RemoteSystem can't be reached using Supported RXA protocols.
```

As stated in the Before you begin information, if Cygwin is present on a remote Windows system that is hosting middleware, errors can occur during Maximo Asset Management installation. This error is displayed during host validation.

```
Aug 3, 2010 9:52:32 AM com.ibm.tivoli.ccmdb.install.common.log.
CmnInstallLogUtils handleUnexpectedException
FINE: ENTER^java.net.ConnectException: CTGRI0023E An error occurred
when executing GET_FREE_PHYS_MEM.
 at com.ibm.tivoli.remoteaccess.UNIXProtocol.
getFreePhysicalMemory(UNIXProtocol.java:1358)
 at com.ibm.tivoli.ccmdb.install.common.util.rxa.RxaHost.
initThreadRemoteAccess(RxaHost.java:434)
 at com.ibm.tivoli.ccmdb.install.common.util.rxa.RxaHost.
initThreadRemoteAccess(RxaHost.java:277)
 at com.ibm.tivoli.ccmdb.install.common.util.rxa.RxaHost.
getRemoteAccess(RxaHost.java:169)
 at com.ibm.tivoli.ccmdb.install.common.util.rxa.RxaUtil.
directoryExists(RxaUtil.java:731)
 at com.ibm.tivoli.ccmdb.install.common.util.validation.
CfgValidateRemoteSystem.directoryExists(CfgValidateRemoteSystem.java:94)
 at com.ibm.tivoli.ccmdb.install.common.config.was.ConfigWasThinClient.
copyTrustStore(ConfigWasThinClient.java:396)
 at com.ibm.tivoli.ccmdb.install.common.config.was.ConfigWasThinClient.
configWasThinClient(ConfigWasThinClient.java:529)
 at com.ibm.tivoli.ccmdb.install.common.config.was.ConfigWasThinClient.
runConfigurationStep(ConfigWasThinClient.java:714)
 at com.ibm.tivoli.ccmdb.install.common.config.TaskRunner.
runSingleTask(TaskRunner.java:324)
 at com.ibm.tivoli.ccmdb.install.foundation.ccmdb.FndUpgradePanelActions.
handleInstall(FndUpgradePanelActions.java:256)
 at com.ibm.tivoli.ccmdb.install.foundation.ccmdb.AFndCustomCodeAction.
install(AFndCustomCodeAction.java:127)
 at com.zerog.ia.installer.actions.CustomAction.installSelf(DashoA10*..)
 at ZeroGad8.run(DashoA10*..)
^T^CTGRI0023E An error occurred when executing GET_FREE_PHYS_MEM.
java.net.ConnectException: CTGRI0023E An error occurred when executing
GET_FREE_PHYS_MEM.
```

In this case, you must either uninstall or disable the SSH daemon (sshd) included with Cygwin.

After you resolve these errors, you can continue to use the Maximo Asset Management installation program.

Application server

SOAP errors

Error details for the failure to deploy the maximo.ear and maximoiehs.ear files can be found in several places, including the CTGInstallTrace00.log file and also the SystemOut.log, SystemError.log, and Trace.log files hosted on the WebSphere Application Server Network Deployment deployment manager.

Typical EAR file deployment failures can include SOAP connection errors where the SOAP port (8879) is not available, or inadequate space on the WebSphere Application Server Network Deployment server to either transfer or deploy the maximo.ear file.

You might encounter a SOAPException error during deployment of the `maximo.ear` or `maximoiehs.ear` from the administrative system to the WebSphere Application Server Network Deployment. Under certain conditions, WebSphere Application Server Network Deployment might be unable to service requests to deploy the maximo or maximohelp applications and a SOAPException occurs.

The following CTGInstallTrace00.log log information is an example of the error information that the program displays when such an exception is encountered.

```
----- START OF LOG FILE INFORMATION

Exception caught during installation of
C:/IBM/SMP/maximo/deployment/default/maximo.ear . Review JVM logs
 in WebSphere,
 install trace logs and wsadmintrace.out for more information
 Exception Type:
 com.ibm.ws.scripting.ScriptingException

Value:  com.ibm.ws.scripting.ScriptingException:
com.ibm.websphere.management.exception.ConfigServiceException

com.ibm.websphere.management.exception.ConnectorException

org.apache.soap.SOAPException: [SOAPException: faultCode=SOAP-ENV:Client;
msg=Error opening socket: java.net.SocketException: Operation timed out:
connect:could be due to invalid address;
targetException=java.lang.IllegalArgumentException: Error opening socket:
java.net.SocketException: Operation timed out: connect:could be due to
invalid address]

----- END OF LOG FILE INFORMATION
```

You might see an error like the previous example in process solution installation log files. These files are contained in the `solutions\logs` subdirectory under the Maximo Asset Management installation. The file names of the log files include the words `Deploy` and `EAR` as part of the filename. Take note of the filepath of the EAR file that was unable to be successfully deployed. In the previous example, the filepath of the EAR file is `C:/IBM/SMP/maximo/deployment/default/maximo.ear`.

The conditions that trigger this problem are often temporary in nature. Check the health of the WebSphere Application Server Network Deployment by attempting to log on to the Deployment Manager using the administrative console. If you are unable to successfully log in, review the WebSphere Application Server Network Deployment log files to determine the nature of the failure.

If you are able to successfully log in, you can attempt to work around this problem by deploying the EAR to WebSphere Application Server Network Deployment using either the administrative console or the `deployApplication.bat` script.

The syntax for the `deployApplication.bat` script follows. Syntax elements in brackets <> need to be replaced with the values for those properties in your environment.

```
install_home\jacl\solutions\DeployApplication.bat
    <WASAdminUserName>
    <WASAdminPassword>
    <ApplicationName> MAXIMO
    <WASNodeName>
    <WASApplicationServerName>
    <path-to-EAR-file>
    <WASVirtualHost>
    <WASWebServerName>
```

So, for example:

```
C:\IBM\SMP\jacl\solutions\DeployApplication.bat" wasadmin <waspassword>
MAXIMO
ctgNode01 MXServer C:\IBM\SMP\maximo\deployment\default\maximo.ear
maximo_host
webserver1
```

Connecting to the application

Near the end of the installation process, the Maximo Asset Management installation program performs a health check to ensure that the deployment was successful. This health check consists of logging on to the application. If it fails, you see the following error:

```
CTGIn2252IW: Cannot connect to process automation engine web app
```

This likely means that the HTTP server is not functional and routing requests or you did not specify the correct port for your environment. This message can also mean that the application was not started correctly. Attempt to log on to the application directly after exiting the installer. If that fails, check the logs of the HTTP server and MXServer on the WebSphere Application Server Network Deployment server to verify that they are up and running.

Note: Port 80 is the HTTPServer port and the value most likely used during installation, assuming that you installed the HTTPServer. If the HTTPServer is installed but not bound to port 80, then use the port that it is bound to. Port 9080 works in a limited number of scenarios. These scenarios include not being deployed on a cluster or if the application server is located on a dmgr system. In most deployments, it is not advisable to use port 9080.

For future use, the port is saved in the Maximo database table maxpropvalue and can be updated to match your environment after the installation is complete.

Database

Updatedb

The updatedb command is run several times during Maximo Asset Management installation. Each time updatedb is run, a time-stamped log file is generated in the `*install_home*\maximo\tools\maximo\log` directory. If you encounter an error attributed to updatedb, refer to the updatedb log with the most recent timestamp for details.

After performing corrective measures, you can complete the deployment with the taskrunner utility.

MAXPRESENTATION update error

While installing Maximo Asset Management, you might encounter a *MAXPRESENTATION* error.

If you receive the following errors during installation, it indicates the presence of database values that are not synchronized.

```
Error: (RECONLINK) Unable to update MAXPRESENTATION - null
java.lang.Exception
Error: (RECONLINK) Unable to update MAXPRESENTATION - null at
psdi.webclient.upgrade.
MXApplyTransactions.saveApplicationDocument(Unknown Source)
```

If you encounter these errors, use the following SQL statements against the database to verify the cause:

```
select maxreserved from maxsequence where tbname = 'MAXPRESENTATION';
select max(maxpresentationid) from maxpresentation;
```

The maxreserved value needs to be greater than or equal to the max(maxpresentationid) value. If it is not, use the following SQL statement to correct it.

```
update maxsequence set maxreserved = (select max(maxpresentationid) from
maxpresentation) where tbname='MAXPRESENTATION' and
name='MAXPRESENTATIONID';
```

Oracle Text indexing

Maximo Asset Management requires a series of text indexes to improve performance of text searches. These are created when the maxinst command is run as part of the installation. If maxinst fails to create text indexes for an Oracle database, errors like the following example in the `CTGInstallTrace.log` file occur:

```
ORA-01031
ORA-04045 with MDSYS.SDO_GEOR_TRUNC_TABLE
```

To resolve the issue, you must install Oracle Spatial:

1. Connect to the database instance by specifying AS SYSDBA
2. Create the MDSYS user with a command in the following format:
   ```
   SQL> CREATE USER MDSYS IDENTIFIED BY <password>;
   ```
3. Grant the required privileges to the MDSYS user by running the following procedure:
   ```
   SQL> @ORACLE_HOME/md/admin/mdprivs.sql
   ```
4. Connect as MDSYS.
5. Install Spatial by running the following procedure:
   ```
   SQL> @ORACLE_HOME/md/admin/catmd.sql
   ```
6. Connect as SYS and lock the MDSYS user account to prevent unauthorized use.
   ```
   SQL> ALTER USER MDSYS ACCOUNT LOCK;
   ```
7. Rebuild the triggers by using the following command:
   ```
   @/<oracle_home>/rdbms/admin/utlprp.sql 0
   ```

Directory server

If you create users and groups manually in Microsoft Active Directory but, during the Maximo Asset Management installation, you select the option to have the installer create the required users, you can receive an error like the following example:

```
Aug 4, 2008 2:17:26 PM
com.ibm.tivoli.ccmdb.install.common.config.was.CfgConfigWebSphere
runJythonScript
INFO: EXIT ^^o^{{ReturnCode: 1
CompletionMessage:
CTGIN2255I: The script
D:\TTEMP\scripts\was\DeploymentManager.py
completed with returncode 1.
StandardOutput: WASX7209I: Connected to process "dmgr" on node
wasundm2Manager using SOAP
connector;  The type of process is: DeploymentManager
WASX7303I: The following options are passed to the scripting environment and
are available as
arguments that are stored in the argv variable: "[vmmUsersAndGroupsExist,
MAXADMIN:mxintadm,maxadmin,
MAXIMOUSERS:mxintadm,maxadmin,maxreg]"
```

```
wasundm2Cell
case:vmmUsersAndGroupsExist, with arguments:['MAXADMIN:mxintadm,maxadmin',
'MAXIMOUSERS:mxintadm,maxadmin,maxreg']
ENTER:vmmUsersAndGroupsExist
args passed  ['vmmUsersAndGroupsExist', 'MAXADMIN:mxintadm,maxadmin',
'MAXIMOUSERS:mxintadm,maxadmin,maxreg']
MAXADMIN:mxintadm,maxadmin
group  MAXADMIN  doesn't exist
EXIT:vmmUsersAndGroupsExist RC= 1
StandardError:
```

To correct this error, clear the Create the required users option shown on the security panel of the Maximo Asset Management installation program. After clearing the option, continue with the installation.

Obsolete and prohibited property values

Deployment details are stored in the database and also on the administrative system in the `install.properties` and `maximo.properties` files.

Obsolete property values

When you install a fix pack or otherwise upgrade an existing ISM product, the installation program uses values recorded from the previous deployment. If you reconfigured any systems used for the original deployment, such as changing a host name, they must be recorded in the `install.properties` and `maximo.properties` files.

If you see the message: `CTGIN2233I WebSphere Node Agent Not Running` in the status bar of the installation program, log on to the WebSphere Application Server Network Deployment administrative console to verify that the node agent is up and running. If you discover it is running, stop and restart the node agent and attempt the installation again. If you still receive this message, chances are it is related to a mismatch between the WebSphere Application Server Network Deployment administrator user ID or password property value originating from the initial deployment and the current value. In this case, you would need to update the property in the install.properties file.

The following errors in the `wsadmin.traceout` file indicate that properties recorded for the initial deployment do not match properties used for the current installation action:

```
javax.management.JMRuntimeException: ADMN0022E: Access is denied for the
getProcessType operation on Server MBean because of insufficient or empty
credentials.
[2/3/09 15:06:24:946 EST] 0000000a AbstractShell A WASX7093I:
Issuing message:
"WASX7246E: Cannot establish "SOAP" connection to host "myhostname.com"
because of an
authentication failure. Ensure that user and password are correct on the
command line or
in a properties file.
Exception message (if any): "ADMN0022E: Access is denied for the
getProcessType operation
on Server MBean because of insufficient or empty credentials.""
```

The following errors in the `CTGInstallTrace00.log` file indicate that properties recorded for the initial deployment do not match used for the current installation action:

```
Input Error: Can not find script file "E:\IBM\SMP\wasclient\sleep.vbs".
WASX7246E: Cannot establish "SOAP" connection to host "myhost.com"
because of an
authentication failure. Ensure that user and password are correct on
the command line
or in a properties file.
FINE: ENTER^^S^CTGIN2233I: WebSphere NodeAgent is not Running.
```

The following error in the Maximo Asset Management installation program also indicates that the property values require updating.

```
CTGIN0210E: Process Solution Installer is unable to access deployment
configuration
properties from the Maximo Database. Ensure that the properties in the
maximo.properties
file are correct and that the Maximo Database is started.
```

To correct these errors, update properties and then complete the deployment using the taskrunner utility.

"Remote configuration enablement" on page 10
The Maximo Asset Management installation program can automatically configure middleware. You must enable a remote access protocol for each system on which you intend to install the middleware.

"General troubleshooting of the product installation program" on page 198
During product installation, you might need to troubleshoot errors that occur within the installation program.

"Updating environment data" on page 182
When you install a second product on the same administrative workstation, or upgrade a single product, the installation program uses values recorded from the previous deployment. These values are stored on the administrative system in the install.properties and maximo.properties files, and also in the database. If you made any environmental changes to any of the systems used for the original deployment, they must be recorded in the install.properties and maximo.properties files. They also must be updated in the database. Typically, these types of changes include changing a host name or updating a password.

Troubleshooting-specific errors of the product installation program

Refer to this information for troubleshooting-specific error conditions that might result from use of the product installation program.

This information is useful to troubleshooting specific errors.

WebSphere Application Server Network Deployment node agent reported as not running

During installation, you experience a failure attributed to the fact that node agent is not running. When checked through the WebSphere Application Server Network Deployment administrative console it is active.

About this task

This error results from the node configuration not matching the cell configuration. Configuration synchronization must occur between the node and the deployment manager for the cell in which the node is configured. This issue generates error WASX7303I, which claims that the node agent is in an inconsistent state. You must synchronize the node configuration.

Procedure

1. Stop the node agent and application servers on all nodes.
2. Run the syncNode command:
   a. Change directory to `WAS_HOME\AppServer\profiles\ctgAppSrv01\bin\`
   b. Run the following command:

      ```
      syncNode[.sh|.bat] hostname port -trace -username user -password password
      ```

      The *hostname* value is the fully qualified host name of the server where the domain manager is running. The *port* value is the SOAP port, for example, 8870.

Troubleshooting the product uninstallation program

Use the troubleshooting information to troubleshoot errors encountered when using the product uninstallation program.

Troubleshooting information is primarily found in log files

Error CTG00001 when performing an uninstall

In certain instances, while performing a product uninstall from the administrative system, you might encounter error `CTG00001 The uninstall was unsuccessful. You must manually uninstall the Maximo product.`

Exit the error message dialog box. To finish the uninstall, manually delete installation directories located under `C:\IBM\SMP\maximo`. Afterward, verify registry entries for the product and process automation engine product are removed. Registry entries can be found under `HKEY_LOCAL_MACHINE/SOFTWARE/IBM/process automation engine` and under the *shortname* of the ISM family product. For example,Maximo Asset Management. Also, depending on the failure, you might need to remove process manager information from the deployment database.

Notices

This information was developed for products and services offered in the U.S.A.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

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

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

For license inquiries regarding double-byte (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan Ltd.
1623-14, Shimotsuruma, Yamato-shi
Kanagawa 242-8502 Japan

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law: INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those websites. The materials at those websites are not part of the materials for this IBM product and use of those websites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Corporation
2Z4A/101
11400 Burnet Road
Austin, TX 78758 U.S.A.

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement or any equivalent agreement between us.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. The sample programs are provided "AS IS", without warranty of any kind. IBM shall not be liable for any damages arising out of your use of the sample programs.

Trademarks

IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at “Copyright and trademark information” at www.ibm.com/legal/copytrade.shtml.

Java and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.

Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.

Microsoft, Windows, and the Windows logo 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.

Index

Printed in USA