Tivoli® IBM Tivoli Asset Discovery for Distributed
Version 7.2

Upgrade Guide

IBM®

SC23-9997-00

Tivoli® IBM Tivoli Asset Discovery for Distributed
Version 7.2

Upgrade Guide

IBM®

SC23-9997-00

Upgrade Guide

This edition applies to version 7.2 of IBM Tivoli Asset Discovery for Distributed and to all subsequent releases and modifications until otherwise indicated in new editions.

Contents

Chapter 1. Planning the Tivoli Asset Discovery for Distributed upgrade

Before starting the upgrade, review the information in this section to learn about hardware and software requirements and other considerations.

Introduction

IBM® Tivoli Asset Discovery for Distributed provides software and hardware inventory information and use monitoring and is the source of inventory data for Tivoli Asset Management for IT. It helps you maintain an up-to-date inventory of the distributed software assets in your IT infrastructure.

Upgrading to Tivoli Asset Discovery for Distributed - the paths

There are three paths for upgrading to IBM Tivoli Asset Discovery for Distributed V7.2.

All of these paths may consist of either automatic or manual steps depending on the size and complexity of the environment. Each upgrade path is covered by a separate section of the documentation.

- Upgrading from Tivoli License Compliance Manager Version 2.3 Fix Pack 5
- Upgrading from License Metric Tool version 7.1
- Upgrading from License Metric Tool version 7.2

Each upgrade path comprises the following actions:

1. Upgrading the database component
   - Automatic process (interactive installer)
   - DB2 version 9.1 or 9.5 is required, so DB2 upgrade may be needed before upgrading the database component
2. Upgrading the administration server component

   Administration server component can be placed on the embedded or stand-alone version of WebSphere Application Server. If the embedded version is used then steps 1 and 2 are performed together using Tivoli Asset Discovery for Distributed 7.2 installer. Otherwise the administration server component of the old version needs to be uninstalled and then Tivoli Asset Discovery for Distributed 7.2 administration server component needs to be deployed manually or with the help of provided sample script.
3. The server needs to be upgraded before or in parallel with the agents upgrade, because Asset Discovery for Distributed 7.2 server supports backward compatibility with Tivoli License Compliance Manager 2.3 Fix Pack 5 agents and 7.1 agents, but Asset Discovery for Distributed 7.2 agents cannot communicate with the older version server.

The path of upgrading from Tivoli License Compliance Manager V2.3 is more complex because there are additional steps that need to be performed:

- Migrating the content of software catalog if customizations were made using Tivoli License Compliance Manager. Customized data needs to be transferred from Tivoli License Compliance Manager to Software Knowledge Base Toolkit and then to Asset Discovery for Distributed.

- Uninstallation of Tivoli License Compliance Manager runtime servers
- Ensuring the continuity of agent-server communication exists by setting up proxy servers, network topology adaptation or reconfiguration of the agents
- Dealing with multiple organizations if they are in place.
- Manual license configuration in Tivoli Asset Management for IT. See the Tivoli Asset Management for IT information center for more details.

Server hardware and software requirements

After reviewing the capacity requirements and planning your server topology, confirm that you meet the system requirements for the various server components.

CPU and memory requirements for the server and database

Ensure that the computer where you are upgrading the Tivoli® Asset Discovery for Distributed server meets the minimal CPU, and memory requirements for the server and database elements.

The requirements are divided into:

- Hardware requirements for environments with up to 5 000 agents.
- Hardware requirements for environments with 5 000 to 45 000 agents.

Table 1. Hardware requirements for environments with up to 5 000 agents.

CPU		
Server	AIX® and Linux®	2 Power4 1.2 GHz
	Linux and Windows® x86, 32 and 64–bit	at least one Intel® Core Solo T1300 1.66 GHz processor
	Solaris SPARC	Sun-Fire-280R 1015 MHz two–way processor
	HP-UX	rp2470, at least two PA-RISC 2.0 650 MHz processors
	Linux on zSeries®	Type 2084, one dedicated processor.
Database	For CPU requirements for DB2® V9.1, see http://www-01.ibm.com/software/data/db2/9/sysreqs.html.	

Memory		
	Server only	1 GB RAM
	Server and database	3 GB RAM

Table 2. Hardware requirements for environments with 5 000 to 45 000 agents.

CPU		
Server	AIX and Linux	At least one Power6 4.7 GHz processor
	Linux x86, 32 and 64–bit	Intel® Xeon® 2.5 GHz, four-way processor
	Solaris SPARC	One SPARC VI, 2150 MHz (4 threads) processor
	HP-UX	rp8420, at least two PA-RISC 2.0 1.0 GHz processors
	Linux on zSeries	Type 2084, two dedicated processors
	Windows x86, 32 and 64–bit	One Dual Core AMD Opteron, 2.6 GHz processor
Database	For CPU requirements for DB2 V9.1, see http://www-01.ibm.com/software/data/db2/9/sysreqs.html.	

Memory		
	Server only	1 GB RAM
	Server and database	4 GB RAM

Space requirements for the server and database

Check if your computer has the required amount of disk space for upgrading server and database

You can upgrade the Tivoli Asset Discovery for Distributed server and database on the same computer, or on two different machines. The table below shows how much space you need depending on your operating system and the components that you are installing on this machine. The space requirements for the server component were measured for the embedded version of WebSphere® Application Server included in the installation package. If you want the Tivoli Asset Discovery for Distributed server to manage a large environment, you must install it on a standalone application server. For more information, refer to the related links section below.

Important: In addition to the space requirements described below, remember to reserve some space for reports from agents. When you sign a report, it is at first generated and stored as an XML file on your hard drive. For large environments and long reporting periods the file can be up to 2 GB in size. If there is not enough free space, signing the report will fail. You can specify the location where the XML file should be generated by editing the **reportPath** parameter in the `system.properties` file.

The requirements below are for upgrade only.

Operating system	Installed components	Directory	Required space
AIX AIX	Server and database without the DB2 prerequisite	Product installation directory	1158 MB
		Database installation directory	459 MB
		/tmp	612 MB
		/etc	under 1 MB
		/var	under 1 MB
	Server only	Product installation directory	1158 MB
		/tmp	612 MB
		/etc	under 1 MB
		/var	under 1 MB
	Database without the DB2 prerequisite	Product installation directory	44 MB
		Database installation directory	under 1 MB
		/tmp	267 MB
		/etc	under 1 MB
		/var	under 1 MB
HP-UX HP-UX	Server and database without the DB2 prerequisite	Product installation directory	938 MB
		Database installation directory	under 1 MB
		/tmp	343 MB
		/etc	under 1 MB
		/var	under 1 MB
		/var/tmp	417 MB
	Server only	Product installation directory	946 MB
		/tmp	343 MB
		/etc	under 1 MB
		/var/tmp	417 MB
	Database without the DB2 prerequisite	Product installation directory	38 MB
		Database installation directory	under 1 MB
		/tmp	343 MB
		/etc	under 1 MB
		/var	under 1 MB
		/var/tmp	under 1 MB

Operating system	Installed components	Directory	Required space
Linux Linux	Server and database without the DB2 prerequisite	Product installation directory	946 MB
		Database installation directory	37 MB
		/tmp	591 MB
		/etc	under 1 MB
		/var	2 MB
		/var/tmp	under 1 MB
	Server only	Product installation directory	954 MB
		/tmp	589 MB
		/etc	under 1 MB
		/var	4 MB
		/var/tmp	under 1 MB
	Database without the DB2 prerequisite	Product installation directory	38 MB
		Database installation directory	37 MB
		/tmp	121 MB
		/etc	under 1 MB
		/var	2 MB
Solaris Solaris	Server and database without the DB2 prerequisite	Product installation directory	951 MB
		/tmp	182 MB
		/var	259 MB
		/var/tmp	259 MB
	Server only	Product installation directory	898 MB
		/tmp	178 MB
		/var	259 MB
		/var/tmp	259 MB
	Database without the DB2 prerequisite	Product installation directory	41 MB
		/tmp	182 MB
		/var	under 1 MB
Windows Windows	Server and database without the DB2 prerequisite	Product installation directory	2119 MB
		DB2 installation directory	470 MB
		/tmp	588 MB
		Database installation directory	under 1 MB
	Server only	Product installation directory	2074 MB
		/tmp	588 MB
	Database without the DB2 prerequisite	Product installation directory	46 MB
		DB2 installation directory	11 MB
		/tmp	121 MB
		Database installation directory	under 1 MB

Software requirements for the server and database

Ensure that the computer where you are installing the Tivoli Asset Discovery for Distributed server runs on one of the supported operating systems, and that all prerequisite software is installed.

Supported operating systems for server and databases

Table 3. Supported versions of AIX

Version	Required level, service packs, patches
6.1	• APAR IZ37466 • When installing the DB2 database on AIX, you also need the xlC.aix*.rte 8.0.0.4 or higher XL C/C++ runtime environment which you can download from http://www-01.ibm.com/software/awdtools/xlcpp/support/
5.3 (64-bit)	

Table 4. Supported versions of HP-UX

Version	Required level, service packs, patches
11i for PA-RISC 11.23 (64-bit, in 32-bit compatibility mode)	

Table 5. Supported versions of Red Hat Enterprise Linux

Version	Required level, service packs, patches
ES/AS/WS 4 for EM64T and AMD64 (64–bit)	compat-libstdc++-33 compat-libstdc++-296-2.96-132.7.2 Both 64-bit and 32-bit versions of the following packages: compat-libstdc++ compat-db-4.1.25-9 xorg-x11-deprecated-libs-6.8.1 or xorg-x11-deprecated-libs-6.8.2 The following 32-bit version packages: pam cracklib-dicts cracklib glib2 libselinux
ES/AS/WS 5 for EM64T and AMD64 (64–bit)	compat-libstdc++-33 compat-libstdc++-296-2.96-132.7.2 Both 64-bit and 32-bit versions of the following packages: compat-libstdc++ compat-db-4.1.25-9 xorg-x11-deprecated-libs-6.8.1 or xorg-x11-deprecated-libs-6.8.2 The following 32-bit version packages: pam cracklib-dicts cracklib glib2 libselinux
ES/AS/WS 4 for Intel x86 (32–bit)	compat-libstdc++-33

Table 5. Supported versions of Red Hat Enterprise Linux (continued)

Version	Required level, service packs, patches
ES/AS/WS 5 for Intel x86 (32–bit)	compat-libstdc++-33
AS, version 4 for IBM iSeries® and pSeries® (64-bit)	compat-libstdc++-33 compat-libstdc++-295-2.95.3-81 Both 64-bit and 32-bit versions of the following packages: compat-libstdc++ compat-db-4.1.25-9 xorg-x11-deprecated-libs-6.8.1 or xorg-x11-deprecated-libs-6.8.2 The following 32-bit version packages: pam cracklib-dicts cracklib glib2 libselinux
AS, version 5 for IBM iSeries and pSeries (64-bit)	compat-libstdc++-33compat-libstdc++-295-2.95.3-81 Both 64-bit and 32-bit versions of the following packages: compat-libstdc++ compat-db-4.1.25-9 xorg-x11-deprecated-libs-6.8.1 or xorg-x11-deprecated-libs-6.8.2 The following 32-bit version packages: pam cracklib-dicts cracklib glib2 libselinux Update 1 or later for LPAR mobility
AS, version 4 for IBM zSeries (64–bit)	compat-libstdc++-33compat-libstdc++-295-2.95.3-81 Both 64-bit and 31-bit versions of the following packages: compat-libstdc++ compat-db-4.1.25-9 xorg-x11-deprecated-libs-6.8.1 or xorg-x11-deprecated-libs-6.8.2 The following 31-bit version packages: pam cracklib-dicts cracklib glib2 libselinux
AS, version 5 for IBM zSeries (64–bit)	Update 1, compat-libstdc++-33compat-libstdc++-295-2.95.3-81 Both 64-bit and 31-bit versions of the following packages: compat-libstdc++ compat-db-4.1.25-9 xorg-x11-deprecated-libs-6.8.1 or xorg-x11-deprecated-libs-6.8.2 The following 31-bit version packages: pam cracklib-dicts cracklib glib2 libselinux

Note: The server and database and their prerequisites require 32-bit support. If you are installing a server or database on a Red Hat Enterprise Linux 64-bit platform, you must ensure that 32-bit support is enabled. In addition to the required packages listed above, you also need to install the Compatibility Architecture Support or Compatibility Architecture Development Support on your system.

Table 6. Supported versions of SUSE Linux Enterprise Server

Version	Required level, service packs, patches
10 for Intel/AMD x86	compat-libstdc++ The following 32-bit version packages: pam cracklib-dicts cracklib glib2 libselinux The following 64-bit version packages: xorg-x11-libs-64bit-6.9.0-50.58.ppc.rpm expat-64bit-2.0.0-13.2.ppc.rpm fontconfig-64bit-2.3.94-18.16.ppc.rpm freetype2-64bit-2.1.10-18.14.ppc.rpm
10 for EM64T and AMD64	
10 for IBM iSeries/pSeries (64-bit)	compat-libstdc++ Service Pack 1 or later for LPAR mobility The following 32-bit version packages: pam cracklib-dicts cracklib glib2 libselinux The following 64-bit version packages: xorg-x11-libs-64bit-6.9.0-50.58.ppc.rpm expat-64bit-2.0.0-13.2.ppc.rpm fontconfig-64bit-2.3.94-18.16.ppc.rpm freetype2-64bit-2.1.10-18.14.ppc.rpm
10 for IBM zSeries (64-bit) on 64-bit hardware	compat-libstdc++ The following 31-bit version packages: pam cracklib-dicts cracklib glib2 libselinux The following 64-bit version packages: xorg-x11-libs-64bit-6.9.0-50.58.ppc.rpm expat-64bit-2.0.0-13.2.ppc.rpm fontconfig-64bit-2.3.94-18.16.ppc.rpm freetype2-64bit-2.1.10-18.14.ppc.rpm

Table 6. Supported versions of SUSE Linux Enterprise Server (continued)

Version	Required level, service packs, patches
9 for Intel x86	Service Pack 3, compat-libstdc++ The following 32-bit version packages: pam cracklib-dicts cracklib glib2 libselinux
9 for EM64T and AMD64	compat-libstdc++ The following 32-bit version packages: pam cracklib-dicts cracklib glib2 libselinux
9 for IBM iSeries/pSeries (64-bit)	Service Pack 3a for iSeriesService Pack 3 for pSeries The following 32-bit version packages: pam cracklib-dicts cracklib glib2 libselinux
9 for IBM zSeries (64-bit)	compat-libstdc++ The following 31-bit version packages: pam cracklib-dicts cracklib glib2 libselinux

Table 7. Supported versions of Sun Solaris

Version	Required level, service packs, patches
10 Operating System for SPARC platforms (64-bit)	
9 Operating System for SPARC platforms (64-bit)	

Table 8. Supported versions of Windows

Version	Required level, service packs, patches
Server 2008 Standard Edition (32-bit and 64-bit) for Intel x86	
Server 2008 Enterprise Edition (32-bit and 64-bit) for Intel x86	
Server 2003 Standard Edition (32-bit and 64-bit)	
Server 2003 Enterprise Edition (32-bit and 64-bit)	

Supported partitioning technologies - servers

Any partitioning technology that runs one of the supported operating systems mentioned above.

Other software prerequisites

Tivoli Asset Discovery for Distributed includes the major software prerequisites, DB2 version 9.1 and WebSphere Application Server version 6.1. You have two options for installing the WebSphere software prerequisite:

- If you do not plan to support more than 5000 agents, you can install an *embedded* version of the WebSphere Application Server from the Asset Discovery for Distributed wizard.
- To support a larger infrastructure, you must install a base version of WebSphere Application Server before installing Asset Discovery for Distributed. You can install the base edition using the V6.1 installation media that are provided with this product, or you can use an existing installation of WebSphere Application Server V6.1 or later. For more details about WebSphere installation, refer to the WebSphere information center.

You have two options for using the DB2 software prerequisite in the upgrade process:

- You can upgrade it ahead of time, using the installation media provided with Asset Discovery for Distributed.
- You can use an existing license of DB2 that you have already installed. Refer to the following table for required software levels.

The following table summarizes additional software prerequisites.

Software		
Server	**Database driver**	
		JDBC driver type 4 is automatically installed if not already present.
	UNIX® shell	
		To install the servers on UNIX platforms you must have the Bourne shell (sh) installed and activated. It is not necessary to run the installation from the Bourne shell. You also need to install and activate the Korn shell.
	Web browser	
		A web browser is required to access the web user interface of the server. It is also needed for the installation launchpad to start; however, it is also possible to start the installation of Tivoli Asset Discovery for Distributed without the launchpad. Supported browsers on different platforms: • **Supported MS Windows versions** – Internet Explorer 6.x, and 7.x, – Firefox 2.0.x • **Other supported platforms** – Firefox 2.0.x **Note:** It is important not to turn the JavaScript™ option off in the browser as some of the functionalities of the web interface might not function properly. For secure connections, cookies need to be enabled.

Software		
Database	**Database server**	
		One of the following versions: • DB2, Enterprise Server Edition server, version 9.5 • DB2, Enterprise Server Edition server, version 9.1 **Note:** 1. The DB2 server must be configured for remote communication - that is to say, the **svcename** parameter needs to be set. 2. You must obtain DB2 9.1 Fix Pack 4 to install on Windows Server 2008 and AIX 6.1 machines.
	UNIX shell	
		To install the databases on UNIX platforms you must have the korn shell (ksh) installed and activated. It needs to be set as the default shell for the DB2 instance owner. **Note:** The shell must be present but the setup command to install the database can be issued from any shell – not necessarily the korn shell.

Supported national languages for the Tivoli Asset Discovery for Distributed server and agents

User Interface is translated into thirteen languages in the 7.2 release of Tivoli Asset Discovery for Distributed.

Table 9. Supported national languages for Tivoli Asset Discovery for Distributed User Interface help and Documentation

Number	Language	User Interface	Documentation (Upgrading)
1	Simplified Chinese	yes	yes
2	Traditional Chinese	yes	no
3	Czech	yes	no
4	French	yes	yes
5	German	yes	yes
6	Hungarian	yes	no
7	Italian	yes	no
8	Japanese	yes	yes
9	Korean	yes	yes
10	Polish	yes	no
11	Portuguese	yes	yes
12	Russian	yes	no
13	Spanish	yes	yes

Agent hardware and software requirements

The topics in this section contain information about hardware and software prerequisites that need to be fulfilled when deploying Tivoli Asset Discovery for Distributed agents.

Software requirements for the agents

Ensure that the machine where you are installing the agent runs on one of the supported operating systems, and that the corequisite software is installed.

Supported operating systems and partitioning technologies

Note: Cloning of virtual machines is not supported for any of the partitioning technologies.

Table 10. Supported versions of IBM AIX

Version	Levels, service packs, patches, compatibility packs	Partitioning technologies
6.1	APAR IZ49636 - this fix is required if you are installing the agent in a WPAR environment. APAR IZ37466 - this fix is required if you are installing the agent in a WPAR environment and using WPAR or LPAR mobility/relocation. To apply the fix for IZ37466, the AIX 6.1 instance needs to be upgraded to Technology Level 3. AIX Technology Level 6100-02-03-0909 or higher is recommended in both LPARs between which a WPAR (with an agent installed) is being relocated.	LPAR PowerVM™ - DLPAR PowerVM - Single Shared Processor Pool PowerVM - Micro-Partitioning™ PowerVM - Multiple Shared Processor Pools PowerVM - Shared Dedicated Processor System WPARs (both regulated and un-regulated, also RSET bound) Application WPARs LPAR mobility WPAR mobility
5.3 (32-bit and 64-bit)	xlC.aix50.rte.6.0.0.3 or later APAR IY51805 Maintenance level 3 to support sub capacity pricing on Power 5 **Note:** Level 3 is a minimum requirement, but use maintenance level 7 to support Multiple Processor Shared Pools. Technology Level 7 or later for LPAR mobility	LPAR PowerVM - DLPAR PowerVM - Single Shared Processor Pool PowerVM - Micro-Partitioning PowerVM - Multiple Shared Processor Pools PowerVM - Shared Dedicated Processor LPAR mobility
5.2 (32-bit and 64-bit)	xlC.aix50.rte.6.0.0.3 or later APAR IY51805	LPAR PowerVM - DLPAR PowerVM - Single Shared Processor Pool

Table 11. Supported versions of IBM i (formerly known as i5/OS)

Version	Levels, service packs, patches, compatibility packs	Partitioning technologies
V6R1	Options 13 and 30 of 5761SS1 PTF SI33108 for 5761SS1 LIC PTF MF46769 (if you are using secure communication)	LPAR PowerVM - DLPAR PowerVM - Single Shared Processor Pool PowerVM - Micro-Partitioning PowerVM - Multiple Shared Processor Pools PowerVM - Shared Dedicated Processor
V5R4	Options 13 and 30 of 5722SS1 PTF SI32724 for 5722SS1 Crypto Access Provider 128-bit, PID: 5722AC3 (if secure communication is to be used)	
V5R3	Options 13 and 30 of 5722SS1 PTF MF34223 to support sub capacity pricing on Power 5 PTF SI33011 for 5722SS1 Crypto Access Provider 128-bit, PID: 5722AC3 (if secure communication is to be used)	LPAR PowerVM - DLPAR PowerVM - Single Shared Processor Pool PowerVM - Micro-Partitioning

Table 12. Supported versions of HP-UX

Version	Levels, service packs, patches, compatibility packs	Partitioning technologies
11i V3 for PA-RISC (64-bit)		nPAR vPAR
11i V11.23 for PA-RISC (64-bit, in 32-bit compatibility mode)	Quality Pack Bundle for HP-UX 11i v2, March 2006	
11i V3 on Itanium® 2 Integrity Server		HP Integrity Virtual Machines nPAR vPAR
11i V11.23 on Itanium 2 Integrity Server	Quality Pack Bundle for HP-UX 11i v2, March 2006	
11i v1 for PA-RISC		nPAR vPAR

Table 13. Supported versions of Red Hat Enterprise Linux

Version	Levels, service packs, patches, compatibility packs	Partitioning technologies
version 5 for AMD64/EAMT64	compat-libstdc++-33	VMware ESX Server 3.0 - Single Server, Cluster, Mobility (VMware Vmotion) VMware ESX Server 3.5 - Single Server, Cluster, Mobility (VMware Vmotion) VMware ESXi 3.5 - Single Server, Cluster, Mobility (VMware Vmotion) Fix Pack 1 VMware ESX Server 4.0 - Single Server, Cluster, Mobility (VMware Vmotion) - supported only through VM manager functionality Fix Pack 1 VMware ESXi Server 4.0 - Single Server, Cluster, Mobility (VMware Vmotion) - supported only through VM manager functionality
ES/AS/WS 5 for Intel/AMD (x86)	compat-libstdc++-33	VMware Server 1.0 VMware ESX Server 2.5 - Single Server, Server Farm, Mobility (VMware Vmotion) VMware ESX Server 3.0 - Single Server, Cluster, Mobility (VMware Vmotion) VMware ESX Server 3.5 - Single Server, Cluster, Mobility (VMware Vmotion) VMware ESXi 3.5 - Single Server, Cluster, Mobility (VMware Vmotion) Fix Pack 1 VMware ESX Server 4.0 - Single Server, Cluster, Mobility (VMware Vmotion) - supported only through VM manager functionality Fix Pack 1 VMware ESXi Server 4.0 - Single Server, Cluster, Mobility (VMware Vmotion) - supported only through VM manager functionality
AS, version 5 for IBM iSeries and pSeries (64-bit)	compat-libstdc++-33 Update 1 or later for LPAR mobility	LPAR PowerVM - DLPAR PowerVM - Single Shared Processor Pool PowerVM - Micro-Partitioning LPAR mobility
AS, version 5 for IBM zSeries (31-bit) on 64-bit hardware	compat-libstdc++-33	LPAR z/VM®
version 4 for AMD64/EAMT64	compat-libstdc++-33	

Table 13. Supported versions of Red Hat Enterprise Linux (continued)

Version	Levels, service packs, patches, compatibility packs	Partitioning technologies
ES/AS/WS 4 for Intel or AMD (x86)	Compatibility packs: 1. libgcc-3.4.3-9 (32-bit) 2. compat-libstdc++-33 (must be installed in the specified order)	VMware Server 1.0 VMware ESX Server 2.5 - Single Server, Server Farm, Mobility (VMware Vmotion) VMware ESX Server 3.0 - Single Server, Cluster, Mobility (VMware Vmotion) VMware ESX Server 3.5 - Single Server, Cluster, Mobility (VMware Vmotion) VMware ESXi 3.5 - Single Server, Cluster, Mobility (VMware Vmotion) Fix Pack 1 VMware ESX Server 4.0 - Single Server, Cluster, Mobility (VMware Vmotion) - supported only through VM manager functionality Fix Pack 1 VMware ESXi Server 4.0 - Single Server, Cluster, Mobility (VMware Vmotion) - supported only through VM manager functionality
AS, version 4 for IBM iSeries and pSeries (64-bit)	Compatibility packs: 1. libgcc-3.4.3-9 (32-bit) 2. compat-libstdc++-33 (must be installed in the specified order)	LPAR PowerVM - DLPAR PowerVM - Single Shared Processor Pool PowerVM - Micro-Partitioning
AS, version 4 for IBM zSeries 64–bit		
AS, version 4 for IBM zSeries (31-bit) on 64-bit hardware	compat-libstdc++-33	LPAR z/VM

Table 14. Supported versions of Red Hat Linux Desktop

Version	Levels, service packs, patches, compatibility packs	Partitioning technologies
version 5 for Intel/AMD (x86)	compat-libstdc++-33	VMware ESX Server 3.0 - Single Server, Cluster, Mobility (VMware Vmotion) VMware ESX Server 3.5 - Single Server, Cluster, Mobility (VMware Vmotion) VMware ESXi 3.5 - Single Server, Cluster, Mobility (VMware Vmotion) Fix Pack 1 VMware ESX Server 4.0 - Single Server, Cluster, Mobility (VMware Vmotion) - supported only through VM manager functionality Fix Pack 1 VMware ESXi Server 4.0 - Single Server, Cluster, Mobility (VMware Vmotion) - supported only through VM manager functionality

Table 14. Supported versions of Red Hat Linux Desktop (continued)

Version	Levels, service packs, patches, compatibility packs	Partitioning technologies
version 4 for Intel/AMD (x86)	compat-libstdc++-33	VMware Server 1.0 VMware ESX Server 2.5 - Single Server, Server Farm, Mobility (VMware Vmotion) VMware ESX Server 3.0 - Single Server, Cluster, Mobility (VMware Vmotion) VMware ESX Server 3.5 - Single Server, Cluster, Mobility (VMware Vmotion) VMware ESXi 3.5 - Single Server, Cluster, Mobility (VMware Vmotion) Fix Pack 1 VMware ESX Server 4.0 - Single Server, Cluster, Mobility (VMware Vmotion) - supported only through VM manager functionality Fix Pack 1 VMware ESXi Server 4.0 - Single Server, Cluster, Mobility (VMware Vmotion) - supported only through VM manager functionality

Table 15. Supported versions of SUSE Linux Enterprise Server

Version	Levels, service packs, patches, compatibility packs	Partitioning technologies
10 for AMD64/EAMT64	compat-libstdc++	VMware ESX Server 3.0 - Single Server, Cluster, Mobility (VMware Vmotion) VMware ESX Server 3.5 - Single Server, Cluster, Mobility (VMware Vmotion) VMware ESXi 3.5 - Single Server, Cluster, Mobility (VMware Vmotion) Fix Pack 1 VMware ESX Server 4.0 - Single Server, Cluster, Mobility (VMware Vmotion) - supported only through VM manager functionality Fix Pack 1 VMware ESXi Server 4.0 - Single Server, Cluster, Mobility (VMware Vmotion) - supported only through VM manager functionality
10 for Intel/AMD (x86)	compat-libstdc++	VMware Server 1.0 VMware ESX Server 3.0 - Single Server, Cluster, Mobility (VMware Vmotion) VMware ESX Server 3.5 - Single Server, Cluster, Mobility (VMware Vmotion) VMware ESXi 3.5 - Single Server, Cluster, Mobility (VMware Vmotion) Fix Pack 1 VMware ESX Server 4.0 - Single Server, Cluster, Mobility (VMware Vmotion) - supported only through VM manager functionality Fix Pack 1 VMware ESXi Server 4.0 - Single Server, Cluster, Mobility (VMware Vmotion) - supported only through VM manager functionality

Table 15. Supported versions of SUSE Linux Enterprise Server (continued)

Version	Levels, service packs, patches, compatibility packs	Partitioning technologies
10 for IBM iSeries/pSeries (64-bit)	compat-libstdc++ Service Pack 1 for LPAR mobility	LPAR PowerVM - DLPAR PowerVM - Single Shared Processor Pool PowerVM - Micro-Partitioning LPAR mobility
10 for IBM zSeries (64-bit) on 64-bit hardware	compat-libstdc++	LPAR z/VM
9 for Intel/AMD (x86)	Service pack 1 to support sub-capacity pricing on Power 5 compat-libstdc++	VMware Server 1.0 VMware ESX Server 2.5 - Single Server, Server Farm, Mobility (VMware Vmotion) VMware ESX Server 3.0 - Single Server, Cluster, Mobility (VMware Vmotion) VMware ESX Server 3.5 - Single Server, Cluster, Mobility (VMware Vmotion) VMware ESXi 3.5 - Single Server, Cluster, Mobility (VMware Vmotion) Fix Pack 1 VMware ESX Server 4.0 - Single Server, Cluster, Mobility (VMware Vmotion) - supported only through VM manager functionality Fix Pack 1 VMware ESXi Server 4.0 - Single Server, Cluster, Mobility (VMware Vmotion) - supported only through VM manager functionality
9 for AMD64/EAMT64		
9 for IBM iSeries/pSeries (64-bit)		LPAR PowerVM - DLPAR PowerVM - Single Shared Processor Pool PowerVM - Micro-Partitioning
9 for IBM zSeries (31-bit and 64-bit)		LPAR z/VM

Table 16. Supported versions of SUSE Linux Enterprise Desktop

Version	Levels, service packs, patches, compatibility packs	Partitioning technologies
10 for Intel/AMD (x86)	compat-libstdc++	VMware Server 1.0 VMware ESX Server 3.0 - Single Server, Cluster, Mobility (VMware Vmotion) VMware ESX Server 3.5 - Single Server, Cluster, Mobility (VMware Vmotion) VMware ESXi 3.5 - Single Server, Cluster, Mobility (VMware Vmotion) Fix Pack 1 VMware ESX Server 4.0 - Single Server, Cluster, Mobility (VMware Vmotion) - supported only through VM manager functionality Fix Pack 1 VMware ESXi Server 4.0 - Single Server, Cluster, Mobility (VMware Vmotion) - supported only through VM manager functionality

Table 17. Supported versions of Novell Linux Desktop

Version	Levels, service packs, patches, compatibility packs	Partitioning technologies
9 for AMD64/EAMT64	compat-libstdc++	VMware Server 1.0 VMware ESX Server 2.5 - Single Server, Server Farm, Mobility (VMware Vmotion) VMware ESX Server 3.0 - Single Server, Cluster, Mobility (VMware Vmotion) VMware ESX Server 3.5 - Single Server, Cluster, Mobility (VMware Vmotion) VMware ESXi 3.5 - Single Server, Cluster, Mobility (VMware Vmotion) Fix Pack 1 VMware ESX Server 4.0 - Single Server, Cluster, Mobility (VMware Vmotion) - supported only through VM manager functionality Fix Pack 1 VMware ESXi Server 4.0 - Single Server, Cluster, Mobility (VMware Vmotion) - supported only through VM manager functionality
9 for Intel/AMD (x86)	compat-libstdc++	VMware ESX Server 2.5 - Single Server, Server Farm, Mobility (VMware Vmotion) VMware ESX Server 3.0 - Single Server, Cluster, Mobility (VMware Vmotion) VMware ESX Server 3.5 - Single Server, Cluster, Mobility (VMware Vmotion) VMware ESXi 3.5 - Single Server, Cluster, Mobility (VMware Vmotion) Fix Pack 1 VMware ESX Server 4.0 - Single Server, Cluster, Mobility (VMware Vmotion) - supported only through VM manager functionality Fix Pack 1 VMware ESXi Server 4.0 - Single Server, Cluster, Mobility (VMware Vmotion) - supported only through VM manager functionality

Table 18. Supported versions of Sun Solaris

Version	Levels, service packs, patches, compatibility packs	Partitioning technologies
10 Operating System for x86 (64-bit)		Containers/Zones
10 Operating System for SPARC (64-bit)		Dynamic System Domains. Solaris in Dynamic System Domains is supported but not for full capacity. Full capacity PVU values will need to be adjusted upward manually for the number of activated cores on the server. Containers/Zones: inside Dynamic System Domains Containers/Zones: node OS
9 Operating System for SPARC (32–bit and 64-bit)	Patches: 113713-03	Dynamic System Domains. Solaris in Dynamic System Domains is supported but not for full capacity. Full capacity PVU values will need to be adjusted upward manually for the number of activated cores on the server.
8 Operating System for SPARC (32–bit and 64-bit)	110934-28 110380-04	

Table 19. Supported versions of Windows

Version	Levels, service packs, patches, compatibility packs	Partitioning technologies
Vista Ultimate (32-bit and 64-bit)		VMware Server 1.0 VMware ESX Server 3.0 - Single Server, Cluster, Mobility (VMware Vmotion) VMware ESX Server 3.5 - Single Server, Cluster, Mobility (VMware Vmotion) VMware ESXi 3.5 - Single Server, Cluster, Mobility (VMware Vmotion) Fix Pack 1 VMware ESX Server 4.0 - Single Server, Cluster, Mobility (VMware Vmotion) - supported only through VM manager functionality Fix Pack 1 VMware ESXi Server 4.0 - Single Server, Cluster, Mobility (VMware Vmotion) - supported only through VM manager functionality
Vista Enterprise (32-bit and 64-bit)		VMware Server 1.0 VMware ESX Server 3.0 - Single Server, Cluster, Mobility (VMware Vmotion) VMware ESX Server 3.5 - Single Server, Cluster, Mobility (VMware Vmotion) VMware ESXi 3.5 - Single Server, Cluster, Mobility (VMware Vmotion) Fix Pack 1 VMware ESX Server 4.0 - Single Server, Cluster, Mobility (VMware Vmotion) - supported only through VM manager functionality Fix Pack 1 VMware ESXi Server 4.0 - Single Server, Cluster, Mobility (VMware Vmotion) - supported only through VM manager functionality

Table 19. Supported versions of Windows (continued)

Version	Levels, service packs, patches, compatibility packs	Partitioning technologies
Vista Business (32-bit and 64-bit)		VMware Server 1.0 VMware ESX Server 3.0 - Single Server, Cluster, Mobility (VMware Vmotion) VMware ESX Server 3.5 - Single Server, Cluster, Mobility (VMware Vmotion) VMware ESXi 3.5 - Single Server, Cluster, Mobility (VMware Vmotion) Fix Pack 1 VMware ESX Server 4.0 - Single Server, Cluster, Mobility (VMware Vmotion) - supported only through VM manager functionality Fix Pack 1 VMware ESXi Server 4.0 - Single Server, Cluster, Mobility (VMware Vmotion) - supported only through VM manager functionality
Server 2008 R2 Standard and Enterprise (64-bit) for Intel x86		VMware ESX Server 3.5 - Single Server, Cluster, Mobility (VMware Vmotion) VMware ESXi 3.5 - Single Server, Cluster, Mobility (VMware Vmotion) Fix Pack 1 VMware ESX Server 4.0 - Single Server, Cluster, Mobility (VMware Vmotion) - supported only through VM manager functionality Fix Pack 1 VMware ESXi Server 4.0 - Single Server, Cluster, Mobility (VMware Vmotion) - supported only through VM manager functionality
Server 2008 Standard and Enterprise (32-bit and 64-bit) for Intel x86		VMware ESX Server 3.5 - Single Server, Cluster, Mobility (VMware Vmotion) VMware ESXi 3.5 - Single Server, Cluster, Mobility (VMware Vmotion) Fix Pack 1 VMware ESX Server 4.0 - Single Server, Cluster, Mobility (VMware Vmotion) - supported only through VM manager functionality Fix Pack 1 VMware ESXi Server 4.0 - Single Server, Cluster, Mobility (VMware Vmotion) - supported only through VM manager functionality
Server 2003 Standard Edition (32-bit and 64-bit)	Service Pack 2	VMware Server 1.0 VMware ESX Server 2.5 - Single Server, Server Farm, Mobility (VMware Vmotion) VMware ESX Server 3.0 - Single Server, Cluster, Mobility (VMware Vmotion) VMware ESX Server 3.5 - Single Server, Cluster, Mobility (VMware Vmotion) VMware ESXi 3.5 - Single Server, Cluster, Mobility (VMware Vmotion) Fix Pack 1 VMware ESX Server 4.0 - Single Server, Cluster, Mobility (VMware Vmotion) - supported only through VM manager functionality Fix Pack 1 VMware ESXi Server 4.0 - Single Server, Cluster, Mobility (VMware Vmotion) - supported only through VM manager functionality
Server 2003 Enterprise Edition (32-bit and 64-bit)	Service Pack 2	
XP Professional	Service Pack 2	

Table 19. Supported versions of Windows (continued)

Version	Levels, service packs, patches, compatibility packs	Partitioning technologies
Windows 2000 Server Windows 2000 Advanced Server	Service Pack 3 or later msvcp60.dll (for installing in interactive and silent mode) The minimum display setting must be at least 256 colors (for installing in interactive mode).	VMware Server 1.0 VMware ESX Server 2.5 - Single Server, Server Farm, Mobility (VMware Vmotion) VMware ESX Server 3.0 - Single Server, Cluster, Mobility (VMware Vmotion) VMware ESX Server 3.5 - Single Server, Cluster, Mobility (VMware Vmotion) VMware ESXi 3.5 - Single Server, Cluster, Mobility (VMware Vmotion) Fix Pack 1 VMware ESX Server 4.0 - Single Server, Cluster, Mobility (VMware Vmotion) - supported only through VM manager functionality Fix Pack 1 VMware ESXi Server 4.0 - Single Server, Cluster, Mobility (VMware Vmotion) - supported only through VM manager functionality Microsoft® Virtual Server 2005
Windows 2000 Professional	Service Pack 3 or later msvcp60.dll (for installing in interactive and silent mode) The minimum display setting must be at least 256 colors (for installing in interactive mode).	VMware Server 1.0 VMware ESX Server 2.5 - Single Server, Server Farm, Mobility (VMware Vmotion) VMware ESX Server 3.0 - Single Server, Cluster, Mobility (VMware Vmotion) VMware ESX Server 3.5 - Single Server, Cluster, Mobility (VMware Vmotion) VMware ESXi 3.5 - Single Server, Cluster, Mobility (VMware Vmotion) Fix Pack 1 VMware ESX Server 4.0 - Single Server, Cluster, Mobility (VMware Vmotion) - supported only through VM manager functionality Fix Pack 1 VMware ESXi Server 4.0 - Single Server, Cluster, Mobility (VMware Vmotion) - supported only through VM manager functionality

Korn shell

If you are installing the agents on a UNIX platform, ensure that the Korn shell is installed and activated.

Tools required to install the agent on a virtual machine

If you are installing the agent in a partitioned environment, you may need to install and activate the virtualization tools required by some partitioning technologies.

Table 20. Partitioning technology prerequisites

Partitioning technology	Tool
VMware Server 1.0 VMware ESX Server 2.5 VMware ESX Server 3.0 VMware ESX Server 3.5 VMware ESXi 3.5 Fix Pack 1 VMware ESX Server 4.0 - supported only through VM manager functionality Fix Pack 1 VMware ESXi Server 4.0 - supported only through VM manager functionality	VMware Tools
Microsoft Virtual Server 2005	Microsoft Virtual Machine Additions
HP Integrity Virtual Machines	**Host operating system** HPVM package **Guest operating system** HPVM-Guest

Software corequisites for agents

Deployment of the agent includes the deployment of corequisite software - Global Security Toolkit , Common Inventory Technology, and, on platforms where virtual machines are not administered by VM managers, also Common Inventory Technology enabler.

Global Security Toolkit is used to provide security between monitoring components. A new version of Global Security Toolkit will be installed by the agent regardless of any versions that may already present on the machine. It cannot be shared by other applications that are installed on this machine.

Note: i5/OS The agent does not install Global Security Toolkit, instead using the version that is already part of the system framework.

Global Security Toolkit		
Operating System	**Version**	**Global Security Toolkit Version**
i5/OS®	V5R3, V5R4, V6R1	6b
Other platforms		7.0.4.14

IBM Tivoli Common Inventory Technology is a component technology used to collect hardware, software, file system, and registry information from systems in a network. Common Inventory Technology might already be deployed for use by other applications on the target computer so the deployment process checks that the installed version is supported for the Asset Discovery for Distributed agent. If the installed version is older than recommended, it is upgraded to the supported one.

Common Inventory Technology enabler is a script that enables the Common Inventory Technology to obtain information about partitioned environments. It is required by the agent on systems not managed by VM managers such as ESX or Virtual Center.

Common Inventory Technology enabler			
Partitioning technology	**Platform**	**Files**	**Subdirectory**
VMWare	Windows	cpuid.exe wenvmw.exe retrieve.pl	`enabler\VMWare\w32-ix86`

	Linux	cpuid
		wenvmw.sh
		retrieve.pl
		dispatcher
			ESX 2.5
			`enabler\VMWare\esx-2.5`
			Other servers
			`enabler\VMWare\linux-ix86`

Microsoft Virtual Server	Windows	cpuid.exe wenmsvs.exe	`enabler\MSVirtualServer`

VMware and Microsoft virtualization considerations

Both the server and agents can be installed in the host and guest operating systems of computers partitioned using VMware and Microsoft virtualization technologies. In the case of agent installation, some technologies require the deployment of the Common Inventory Technology enabler.

Due to the nature of the VMware and Microsoft Virtual Server virtualization technologies, agents deployed on them are not able to gather data about the host computer systems. Therefore, they are not able to gather and send information about, for example, processor types or number of processor cores. Without this kind of information, it is impossible to calculate processor value unit (PVU) capacity for a given software.

To prevent this, you can use a *virtual machine manager* to administer your virtual machines. VM managers are used to collect some additional information concerning virtual machines that are installed in your infrastructure, and they allow the server to process the data collected by the agents. Connecting to a VM manager is the recommended solution for Tivoli Asset Discovery for Distributed.

You can also schedule the Common Inventory Technology enabler script to run on the host at regular intervals to detect any changes in the configuration of partitions. This method is only recommended if you are not using VM manager or your machine cannot be connected to a virtual machine manager.

Common Inventory Technology enabler is required on partitions not managed by a virtual machine manager for the following virtualization technologies:

- Microsoft Virtual Server
- VMware ESX Server 3.5
- VMware ESX Server 3.0
- VMware ESX Server 2.5
- VMware Server 1.0.

On VMware ESX Server 2.5, 3.0 and 3.5 the enabler can also be run on partitions which are managed through a server using VMware Virtual Center. However, it is recommended to use the VM manager in those cases.

Important: You have to use VM managers in cluster environments to ensure that the virtual machine hierarchy is built correctly. Note that in such situations, you

should not use Common Inventory Technology enabler because it cannot provide complete information about cluster topology.

Disk space requirements

Before deploying the Tivoli Asset Discovery for Distributed agents, and the WebSphere agent, ensure that your machine has the required amount of disk space.

For all agent deployment methods, a space check is made to ensure that the installation will not start and then fail because of lack of sufficient space in the agent installation directory. If the space available is insufficient, the installation fails with return code -17.

Table 21. Tivoli Asset Discovery for Distributed agent space requirements

Operating system	Directory	Space required
AIX	Agent installation directory (default: `/var/itlm`)	55 MB
	WebSphere agent directory (additional space in agent installation directory)	230 MB
	Temporary directory (default: `/tmp`)	70 MB
	`Tivoli_Common_Directory``/COD`	10 MB
	SWDCLI registry directory (default: `/.swdis`)	35 MB
	Directory for configuration files (default: `/etc`)	under 1 MB
	Common Inventory Technology (default directory: `/opt/tivoli/cit`)	30 MB
	Common Inventory Technology cache files (default: `/opt/tivoli/cit/cache_data/__username`)	Depends on the number of files, directories, and subdirectories to be scanned. Can be estimated by multiplying the number of files to be scanned by 40 bytes.

Table 21. Tivoli Asset Discovery for Distributed agent space requirements (continued)

HP-UX on PA-RISC	Agent installation directory (default: `/var/itlm`)	85 MB
	WebSphere agent directory (additional space in agent installation directory)	200 MB
	Temporary directory (default: `/tmp`)	80 MB
	Tivoli_Common_Directory`/COD`	10 MB
	SWDCLI registry directory (default: `/.swdis`)	35 MB
	Directory for configuration files (default: `/etc`)	under 1 MB
	Common Inventory Technology (default directory: `/opt/tivoli/cit`)	30 MB
	Common Inventory Technology cache files (default: `/opt/tivoli/cit/cache_data/__username`)	Depends on the number of files, directories, and subdirectories to be scanned. Can be estimated by multiplying the number of files to be scanned by 40 bytes.
HP-UX on Itanium 2 Integrity Server	Agent installation directory (default: `/var/itlm`)	130 MB
	WebSphere agent directory (additional space in agent installation directory)	200 MB
	Temporary directory (default: `/tmp`)	130 MB
	Tivoli_Common_Directory`/COD`	10 MB
	SWDCLI registry directory (default: `/.swdis`)	55 MB
	Directory for configuration files (default: `/etc`)	under 1 MB
	Common Inventory Technology (default directory: `/opt/tivoli/cit`)	50 MB
	Common Inventory Technology cache files (default: `/opt/tivoli/cit/cache_data/__username`)	Depends on the number of files, directories, and subdirectories to be scanned. Can be estimated by multiplying the number of files to be scanned by 40 bytes.

Table 21. Tivoli Asset Discovery for Distributed agent space requirements (continued)

i5/OS	Agent installation directory	80 MB
	WebSphere agent directory in agent installation directory	150 MB
	Temporary directory (default: `/tmp`)	130 MB
	`Tivoli_Common_Directory``/COD`	10 MB
	Common Inventory Technology (default directory: `/opt/tivoli/cit`)	55 MB
	Common Inventory Technology cache files (default: `/opt/tivoli/cit/cache_data/__username`)	Depends on the number of files, directories, and subdirectories to be scanned. Can be estimated by multiplying the number of files to be scanned by 40 bytes.
Linux x86	Agent installation directory (default: `/var/itlm`)	40 MB
	WebSphere agent directory (additional space in agent installation directory)	200 MB
	Temporary directory (default: `/tmp`)	50 MB
	`Tivoli_Common_Directory``/COD`	10 MB
	SWDCLI registry directory (default: `/root/.swdis`)	20 MB
	Directory for configuration files (default: `/etc`)	under 1 MB
	Common Inventory Technology	30 MB
	Common Inventory Technology cache files (default: `/opt/tivoli/cit/cache_data/__username`)	Depends on the number of files, directories, and subdirectories to be scanned. Can be estimated by multiplying the number of files to be scanned by 40 bytes.

Table 21. Tivoli Asset Discovery for Distributed agent space requirements (continued)

Linux pSeries	Agent installation directory (default: `/var/itlm`)	40 MB
	WebSphere agent directory (additional space in agent installation directory)	200 MB
	Temporary directory (default: `/tmp`)	50 MB
	`Tivoli_Common_Directory``/COD`	10 MB
	SWDCLI registry directory (default: `/root/.swdis`)	20 MB
	Directory for configuration files (default: `/etc`)	under 1 MB
	Common Inventory Technology	30 MB
	Common Inventory Technology cache files (default: `/opt/tivoli/cit/cache_data/__username`)	Depends on the number of files, directories, and subdirectories to be scanned. Can be estimated by multiplying the number of files to be scanned by 40 bytes.
Linux zSeries	Agent installation directory (default: `/var/itlm`)	100 MB
	WebSphere agent directory (additional space in agent installation directory)	200 MB
	Temporary directory (default: `/tmp`)	60 MB
	`Tivoli_Common_Directory``/COD`	10 MB
	SWDCLI registry directory (default: `/root/.swdis`)	25 MB
	Directory for configuration files (default: `/etc`)	under 1 MB
	Common Inventory Technology	30 MB
	Common Inventory Technology cache files (default: `/opt/tivoli/cit/cache_data/__username`)	Depends on the number of files, directories, and subdirectories to be scanned. Can be estimated by multiplying the number of files to be scanned by 40 bytes.

Table 21. Tivoli Asset Discovery for Distributed agent space requirements (continued)

Solaris on x86	Agent installation directory (default: `/var/itlm`)	50 MB
	WebSphere agent directory (additional space in agent installation directory)	200 MB
	Temporary directory (default: `/tmp`)	55 MB
	`Tivoli_Common_Directory``/COD`	10 MB
	SWDCLI registry directory (default: `/opt/Tivoli/swdis`)	25 MB
	Directory for configuration files (default: `/etc`)	under 1 MB
	Common Inventory Technology (default directory: `/opt/tivoli/cit`)	25 MB
	Common Inventory Technology cache files (default: `/opt/tivoli/cit/cache_data/__username`)	Depends on the number of files, directories, and subdirectories to be scanned. Can be estimated by multiplying the number of files to be scanned by 40 bytes.
Solaris on SPARC	Agent installation directory (default: `/var/itlm`)	55 MB
	WebSphere agent directory (additional space in agent installation directory)	200 MB
	Temporary directory (default: `/tmp`)	65 MB
	`Tivoli_Common_Directory``/COD`	10 MB
	SWDCLI registry directory (default: `/.swdis`)	25 MB
	Directory for configuration files (default: `/etc`)	under 1 MB
	Common Inventory Technology (default directory: `/opt/tivoli/cit`)	25 MB
	Common Inventory Technology cache files (default: `/opt/tivoli/cit/cache_data/__username`)	Depends on the number of files, directories, and subdirectories to be scanned. Can be estimated by multiplying the number of files to be scanned by 40 bytes.

Table 21. Tivoli Asset Discovery for Distributed agent space requirements (continued)

Windows	Agent installation directory (default: `%WINDIR%/itlm`).	35 MB
	WebSphere agent directory (additional space in agent installation directory)	200 MB
	Temporary directory (default: `%TEMP%`)	30 MB
	`Tivoli_Common_Directory``/COD`	10 MB
	SWDCLI registry directory (default: `C:\swdis`)	10 MB
	Directory for configuration files (default: `%WINDIR%`)	under 1 MB
	Common Inventory Technology (default directory: `C:\Program Files\tivoli\cit`)	10 MB
	Common Inventory Technology cache files (default: `/opt/tivoli/cit/cache_data/__username`)	Depends on the number of files, directories, and subdirectories to be scanned. Can be estimated by multiplying the number of files to be scanned by 40 bytes.

Supported environments for J2EE application monitoring

The Tivoli Asset Discovery for Distributed agent has a subagent that is responsible for monitoring J2EE applications.

The WebSphere agent supports the following versions of WebSphere:

- WebSphere Application Server, version 7.0
- WebSphere Application Server, version 6.1 (excluding versions with fix packs 6.1.0.11 and 6.1.0.13)
- WebSphere Application Server, version 6.0
- WebSphere Application Server, version 5.1
- WebSphere Application Server, version 5.0
- WebSphere Portal, version 6.1
- WebSphere Portal, version 6.0
- WebSphere Portal, version 5.1
- WebSphere Portal, version 5.0

The WebSphere agent supports the following editions of the above mentioned versions of WebSphere:

- WebSphere Application Server, Network Deployment edition
- WebSphere Application Server, Base edition

When WebSphere Portal is installed, the file `itlm.product` exists in the *`WebSphere_Portal_Root`*`\version` directory. This fie contains entries that identify

WebSphere portal products and versions. For WebSphere Portal 5.0 and 5.1, to enable Tivoli Asset Discovery for Distributed monitoring of products that you have installed on WebSphere portal, you must edit the file and uncomment the lines that relate to version of your WebSphere Portal. For WebSphere Portal 6.0 and higher, it is enough to verify that the `itlm.product` file exists.

The WebSphere Application Server agent is automatically installed on monitored computers when a supported version of the WebSphere Application software is present.

Support for high availability environments

This topic provides information about the conditions in which monitoring of high availability environments, managed by IBM High Availability Cluster Multiprocessing, has been validated.

Tivoli Asset Discovery for Distributed agent is able to collect both use and install information about products running within high availability clusters managed by High Availability Cluster Multiprocessing.

The following scenarios have been validated:

High Availability Cluster Multiprocessing configurations

- Hot StandBy
- Mutual Takeover
- Concurrent Access with or without IBM General Parallel File System

High Availability Cluster Multiprocessing Policy

- Rotating

Tivoli Asset Discovery for Distributed configuration

Agents installed on each node that is participating in the cluster, communicating correctly with servers, and not involved in any high availability switching.

Applications

Running on the local node with binaries located in file systems that are visible to High Availability Cluster Multiprocessing or by General Parallel File System as local files.

Supported software installed in High Availability environments is properly detected by Asset Discovery for Distributed, which means that processor value unit consumption is calculated. If your software agreement allows for reduced processor value unit consumption (e.g. in case of Hot StandBy), you can disable PVU calculation for your software installed in High Availability Cluster Multiprocessing environment by excluding one or more software instances.

Supported national languages for i5/OS agents

You must install one of the supported languages as your primary or secondary language on the i5/OS node.

Installed languages on i5/OS		
	Language code	**Language**
	2924	English
	2928	French
	2929	German

Installed languages on i5/OS		
	2931	Spanish
	2932	Italian
	2962	Japanese
	2975	Czech
	2976	Hungarian
	2978	Polish
	2979	Russian
	2980	Portuguese (Brazil)
	2986	Korean
	2987	Traditional Chinese
	2989	Simplified Chinese

Topology and capacity planning

Before installing Tivoli Asset Discovery for Distributed to monitor the installed software in your organization, you need to determine what additional server software you need, based on the size of your IT infrastructure, and how large the database might grow.

Scan groups

Scan groups are units for grouping agents. Scans of installed software and hardware are scheduled on a scan group level. Decide how you want to divide agents between scan groups so that the operations which you can perform by scan groups are meaningful within your organization. Each agent must be assigned to a scan group.

Note: Creating scan groups is not mandatory but preferable. There is always a default scan group to which agents are assigned by default.

Placement of server components

For performance reasons, it is recommended that you install the server software on a dedicated computer. You can install the database on the same computer as the server or on a different one. If you are installing the database on a different computer than the server, you must run the installer twice on both computers.

Depending on the size of your IT infrastructure, you need to make the following choices:

- If you will support fewer than 5000 agents, you can install the limited-use version of WebSphere Application Server software that is embedded with Asset Discovery for Distributed.
- If you will support more than 5000 agents, it is recommended that you install base WebSphere Application Server version 6.1 or higher on the computer where you will install the Asset Discovery for Distributed server. One instance of WebSphere Application Server can support up to 45000 agents.

Placement of agents

In a partitioned operating environment, you must install agents on every guest operating system that hosts the software products for which you need to monitor license compliance.

Agent backward compatibility

The following versions of Tivoli Asset Discovery for Distributed agents are able to connect to the Tivoli Asset Discovery for Distributed 7.2 server:

- 7.1 GA, and fix pack 1
- Tivoli License Compliance Manager 2.3 fix pack 4, 5, 6, and 7

Using secure communications

The use of secure communications between the infrastructure elements is described fully in the "Security" section of the information center.

Network planning

Tivoli Asset Discovery for Distributed and its agents do not generate heavy data traffic for extended periods of time. However, some network planning is required.

If the database is installed on a separate computer from the monitoring server, provide a high-speed connection between the two.

Secure communication can have an impact both on network traffic and server performance, especially on the maximum security level.

Tivoli Asset Discovery for Distributed uses the following ports for the data exchange between the server and its agents.

Note: The ports below are only the default values and can be changed during the installation.

Table 22. Ports used by Tivoli Asset Discovery for Distributed

Type	Value
User Interface	8899 (http) and 8888 (https) These ports are default ports for embedded WebSphere Application Server. If you are not using default ports, you can check the port values in *Installation_folder*/admin/master.tag. For the base version of WebSphere Application Server, the port numbers are characteristic for the profile on which the product is deployed.
Agent-server communication	9988 (http), 9999 (https) and 9977 (https with client authentication)
Database (DB2)	default value of 50000 For information about configuring DB2 ports see http://publib.boulder.ibm.com/infocenter/db2luw/v9/topic/com.ibm.db2.udb.uprun.doc/doc/t0004727.htm.

Security considerations

There are some security issues that you need to take into consideration while installing and configuring the Tivoli Asset Discovery for Distributed.

Required access privileges for the installation

In order to install the Tivoli Asset Discovery for Distributed server or agent you need to log on to the computer where you want to install the software as a user with administrative rights on Windows or as a root on Unix platforms. The only exception to this rule is if you are installing agents using IBM Tivoli Configuration Manager.

Database user IDs

During the installation process, you need to specify a user ID and password for performing DB2 administrative tasks, such as creating and dropping databases. You also need to provide a password for the tlmsrv ID, which is used by server processes to access the database.

Levels of security

There are three possible levels of security used for communication between the server and agents. You need to select one of them depending on the security regulations in your organization.

Minimum
The agent communicates with the server computer on the unsecure port and no check of the client or server identity is made.

Medium
The agent communicates on the secure port and an SSL certificate is used to authenticate the identity of the server.

Maximum
The server must authenticate all clients that contact it. Therefore, all agents that communicate with the server must also be configured for maximum security and must have personal certificates deployed. The server listens on the secure port and the secure port is configured to require both client and server authentication.

Security-Enhanced Linux

Security-Enhanced Linux set to enforcing mode can cause problems with the installation and use of Tivoli Asset Discovery for Distributed server and agents. If your operating system enables SELinux, you will need to either set it to permissive, or disable it completely.

Chapter 2. Upgrading to Tivoli Asset Discovery for Distributed version 7.2

After you have analyzed hardware and software requirements for your Tivoli Asset Discovery for Distributed infrastructure and have read other topology-related important considerations, you are ready to start upgrading the product. Upgrade the server performing the steps provided in the section that contains information regarding your chosen upgrade path, next upgrade the agents and finally configure the server for optimal performance.

Performing pre-upgrade tasks

Prepare the product files and other software components before you begin the upgrade process. You will also probably need to check the version of software components such as WebSphere Application Server or DB2.

Software packages for upgrading to IBM Tivoli Asset Discovery for Distributed 7.2

To perform the upgrade, you need several packages that you can download from the Passport Advantage® or Software Support web site (fix pack) or copy from the product DVD. Some of the images may differ depending on whether you upgrade on the embedded or stand-alone WebSphere Application Server. You will also need fix pack files which are required for bringing WebSphere Application Server to a required software level.

Table 23. Upgrade packages for upgrading on the embedded and stand-alone WebSphere Application Server

No	Type of image	If you upgrade on embedded WebSphere Application Server	If you upgrade on the stand-alone WebSphere Application Server
1.	Server images	• Tivoli Asset Discovery for Distributed 7.2 Server Installation Package Platform Specific • Base Package for Server Installation (must be unzipped in the same directory as the platform-specific server package)	• Tivoli Asset Discovery for Distributed 7.2 Server Installation Package Platform Specific • Base Package for Server Installation (must be unzipped in the same directory as the platform-specific server package) You require the interactive installer because you need to start it to extract the files for manual upgrade.
2.	Agent images	• Tivoli Asset Discovery for Distributed 7.2 Agent Installation Package (native installer) • Agent Installation Package, collection of Software Package Blocks only for Tivoli Configuration Manager-based installation • Common Inventory Technology Enabler	

Table 23. Upgrade packages for upgrading on the embedded and stand-alone WebSphere Application Server (continued)

No	Type of image	If you upgrade on embedded WebSphere Application Server	If you upgrade on the stand-alone WebSphere Application Server
3.	WebSphere Application Server images	• The embedded WebSphere Application Server V6.1 is packaged with the Tivoli Asset Discovery for Distributed 7.2 Server Installation Package • Integrated Solutions Console version 7.1.0.7 Package for Embedded Websphere Application Server IBM Update Installer V7.0.0.7 for WebSphere Software is available on the following download page or on the product DVD, in the directory `server/fixpacks`. If you are upgrading on the embedded WebSphere Application Server, you do not need to install the fix packs - they are installed together with the application server (Fix packs for embedded WebSphere Application Server are shipped within the Server Installation Package.).	• WebSphere Application Server V6.1 (32 or 64-bit) • WebSphere Application Server V6.1 Supplements, which contain: – IBM HTTP Server – Web Server Plug-ins – Migration Tool – IBM Support Assistant – Update Installer • Integrated Solutions Console version 7.1.0.7 Package for Websphere Application Server IBM Update Installer V7.0.0.7 for WebSphere Software is available on the following download page or on the product DVD, in the directory `server/fixpacks`. WebSphere Application Server V6.1.0 fix pack 23 is available on the following download page. Integrated Solutions Console V7.1.0, fix pack 7 is available on the product DVD in the directory `server/fixpacks`.
4.	DB2 images	• DB2 Enterprise Server Edition V9.1 (32 or 64-bit) • DB2 Enterprise Server Edition V9.1 Restricted Use Activation	
5.	Documentation images	• Quick Start Guide • V7.2.0 Quick Start (this image contains complete infocenter) • WebSphere Application Server V6.1 Quick Start CD Guide • DB2 Information Center V9.1 for 32-bit and 64-bit • DB2 Information Center V9.1 Updates for Windows and Linux • PDF Documentation CD DB2 V9.1 English, Brazilian Portuguese, French, German, Italian, and Spanish • PDF Documentation CD DB2 V9.1 English, Bulgarian, Croatian, Czech, Dutch, Hungarian, Portuguese, Romanian, Slovakian, Slovenian • PDF Documentation CD DB2 V9.1 English, Danish, Finnish, Norwegian, Polish, Russian, Swedish • PDF Documentation CD DB2 V9.1 English, Japanese, and Korean • PDF Documentation CD DB2 V9.1 English, Simplified Chinese, and Traditional Chinese	
6.	Additional images for Tivoli Asset Discovery for Distributed	• IBM Tivoli Common Reporting V1.2.0.1 • Tivoli Asset Discovery for Distributed 7.2 reports package for Tivoli Common Reporting	

Preparing files for upgrade

If you downloaded the installation image from Passport Advantage, unpack the files before upgrading the product.

Preparing server files

1. Copy the following files to the server machine:
   - `<INSTALLER_BASE_COMPRESSED_FILE_NAME>.zip`. This package contains platform-independent part of the installation image.
   - `<INSTALLER_COMPRESSED_FILE_NAME>.zip`. This package contains platform-specific part of the installation image.
2. Extract the `<INSTALLER_BASE_COMPRESSED_FILE_NAME>.zip` file.
3. Unpack the file `<INSTALLER_COMPRESSED_FILE_NAME>.zip` to the same directory to which you extracted the `<INSTALLER_BASE_COMPRESSED_FILE_NAME>.zip` file.

Preparing DB2 files

1. Unpack the DB2_ESE_Restricted_Activation_V91.zip file.
2. Depending on your operating system, copy the relevant file into the disk1 directory that has been created in the previous step:
   - for Windows 32bit, C13KRML.exe
   - for Windows 64 bit, DB2_ESE_V913_WINX64.
   - for Linux x86, DB2_ESE_V913_LNXX86.tar
   - for Linux x86 64bit, DB2_ESE_V913_LNXX86_64.tar
   - for Linux PPC, DB2_ESE_V913_LNXPPC.tar
   - for Linux s390, DB2_ESE_V913_LNXS390X.tar
   - for Solaris, DB2_Enterprise_Svr_Ed_Solaris_SPARC.tar
   - for HP-UX, DB2_Enterprise_Svr_Ed_HP-UX_RISC.tar
3. Unpack the file.
4. Specify the disk1 directory as the IBM DB2 setup location.

Checking the version of Tivoli Asset Discovery for Distributed components

Before you start the upgrade process, check the versions of components that are to be upgraded together with Asset Discovery for Distributed.

Checking the version of WebSphere Application Server

Check the version of WebSphere Application Server before you start the upgrade process.

1. Start the operating system command line interface.
2. Enter the following command:
   - UNIX *WAS_PATH* /bin/versionInfo.sh
   - Windows *WAS_PATH* \bin\versionInfo.bat

   You should receive a confirmation which might look like the following one (Windows operating system):

```
C:\Program Files\IBM\WebSphere2\AppServer\bin>versionInfo.bat
WVER0010I: Copyright (c) IBM Corporation 2002, 2005; All rights reserved.
WVER0012I: VersionInfo reporter version 1.15.4.3, dated 11/12/08

--------------------------------------------------------------------------------

IBM WebSphere Application Server Product Installation Status Report
--------------------------------------------------------------------------------


Report at date and time December 3, 2009 10:06:16 AM CET
```

```
Installation
------------------------------------------------------------------------------

Product Directory C:\Program Files\IBM\WebSphere2\AppServer
Version Directory C:\Program Files\IBM\WebSphere2\AppServer\properties\ve
rsion
DTD Directory C:\Program Files\IBM\WebSphere2\AppServer\properties\ve
rsion\dtd
Log Directory C:\Program Files\IBM\WebSphere2\AppServer\logs
Backup Directory C:\Program Files\IBM\WebSphere2\AppServer\properties\ve
rsion\nif\backup
TMP Directory C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\1

Product List
------------------------------------------------------------------------------

BASE installed

Installed Product
------------------------------------------------------------------------------

Name IBM WebSphere Application Server
Version 6.1.0.23
ID BASE
Build Level cf230910.10
Build Date 3/10/09

------------------------------------------------------------------------------

End Installation Status Report
------------------------------------------------------------------------------
```

You have obtained information regarding the version of installed WebSphere Application Server.

Checking the version of Integrated Solutions Console

Check the version of Integrated Solutions Console before you start the upgrade process.

1. Locate the following file in the file system of the server on which Tivoli Asset Discovery for Distributed is installed:
   - UNIX *WAS_PATH*/systemApps/isclite.ear/isclite.war/WEB-INF/config/isc.version.properties
   - Windows *WAS_PATH*\systemApps\isclite.ear\isclite.war\WEB-INF\config\isc.version.properties
2. Open the file in a text editor. In the file, locate the following section:

   ```
   isc.name=Integrated Solutions Console Advanced Edition
   isc.version=7.1.0.7
   isc.release.name=ISC61.WWEBUI
   isc.build.level=f0917.04
   isc.build.date=20090501
   ```

   Line **isc.version=7.1.0.7** contains the version number of installed Integrated Solutions Console. If the version is lower than 7.1.0.7, you need to update it.

Checking the version of DB2

Check the version of DB2 before you start the upgrade process.

1. Start the DB2 command line interface:
   - UNIX Type db2.

- Windows Click **Start** → **Programs** → **IBM DB2** → *Copy Name* → **command line tools**.

  A command line window opens.

2. Check the DB2 version by entering the following command:
   - UNIX su - *instance_owner_name* -c db2level
   - Windows db2level

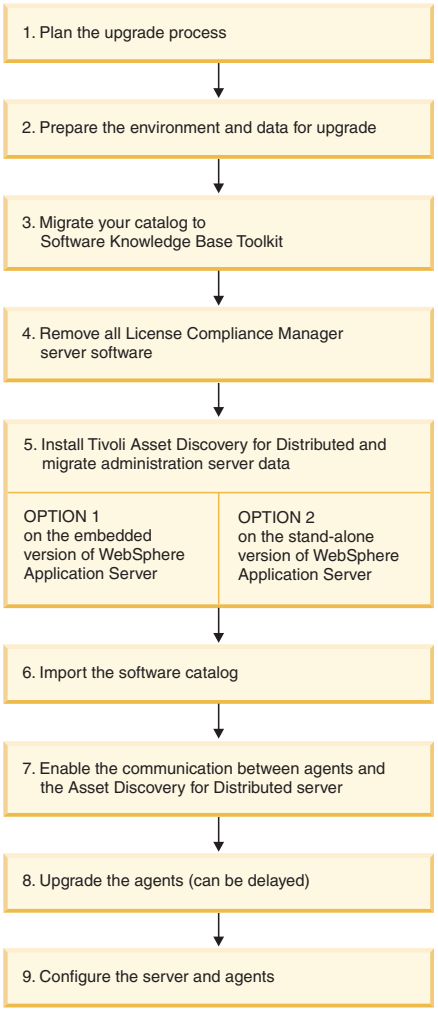
   You should receive a confirmation which might look like the following one (Windows operating system):

```
C:\Program Files\IBM\SQLLIB\BIN>db2level
DB21085I  Instance "DB2" uses "32" bits and DB2 code release "SQL09050" with
level identifier "03010107".
Informational tokens are "DB2 v9.5.0.808", "s071001", "NT3295", and Fix Pack
"0".
Product is installed at "C:\PROGRA~1\IBM\SQLLIB" with DB2 Copy Name "DB2COPY1".
```

Upgrading from Tivoli License Compliance Manager v2.3

The upgrade from Tivoli License Compliance Manager to Tivoli Asset Discovery for Distributed comprises multiple stages. First, you uninstall the runtime servers and their databases, then the administration server. Next you upgrade DB2, migrate the data, install the Asset Discovery for Distributed software, and import the software catalog. If you decide to upgrade the agents but not re-configure them, you will have to set up proxy servers that will forward the data to the Asset Discovery for Distributed server, or re-configure the agents to connect directly to the new Asset Discovery for Distributed server.

Note: The License Compliance Manager v2.3 server with security level set to Medium is able to communicate with agents with security set to Minimum. Bear in mind that after upgrading License Compliance Manager v2.3 to Asset Discovery for Distributed v7.2 it is no longer possible because the server manages the agents only with the same or higher level of security.



To upgrade to Asset Discovery for Distributed, perform the following tasks:

1. Plan the upgrade. This step includes topology planning, for example selection and placement of application server and database components based on the number of agents that you will need to deploy.
2. Prepare the environment and data for upgrade.
3. If you customized the software catalog in Licence Compliance Manager, for example to create or change signatures, migrate your catalog.
4. Shut down and remove all Licence Compliance Manager servers.
5. Install the server and migrate the Tivoli License Compliance Manager database.
6. Import the software catalog.
7. Enable the communication between agents and the Asset Discovery for Distributed server by installing proxy servers in your infrastructure. As an option, you might want to reconfigure agents or change host names in your Domain Name Services server.
8. Upgrade the agents. After agents are upgraded, they will be able to directly connect to the Asset Discovery for Distributed server, so you can remove proxy servers or any configurations you may have done.
9. Configure the server and agents. For information on configuring see Chapter 3, “Configuring Tivoli Asset Discovery for Distributed,” on page 157.

Introduction

Tivoli Asset Discovery for Distributed is a modern replacement for some functionalities provided by Tivoli License Compliance Manager V2.3. It is important to read and understand what the new product brings in relation to License Compliance Manager and how it relates to the other products in the Tivoli Asset Management for IT family.

Tivoli Asset Discovery for Distributed is a new IBM product with the current IBM technology implemented and redesigned user interface. It - together with other Tivoli Asset Management for IT products - provides the same and even more functions than License Compliance Manager does and is built on stronger foundation: industry-recognized, renowned products such as new, version 6.1 Base WebSphere Application Server, DB2 version 9.1 and user-friendly, easily navigable web user interface framework - V7.1.0. Integrated Solutions Console. Follow the links below to learn more about the changes brought about by Asset Discovery for Distributed server (and IBM License Metric Tool).

1. “Reasons to upgrade from Tivoli License Compliance Manager” on page 41
2. “Architectural differences” on page 42
3. “Terminology changes between Tivoli License Compliance Manager and Tivoli Asset Discovery for Distributed” on page 45

Reasons to upgrade from Tivoli License Compliance Manager

Asset Discovery for Distributed provides information about installed hardware and software, and limited software use, for distributed platforms. Thanks to numerous new features and enhancements it is a solid replacement for Tivoli License Compliance Manager.

There are many factors and reasons for upgrading from Tivoli License Compliance Manager to IBM Tivoli Asset Discovery for Distributed. Consider the following facts and benefits that you might enjoy after upgrading to the redesigned and improved software that serves the most important needs in managing software assets.

1. A modern replacement for Tivoli License Compliance Manager

Asset Discovery for Distributed performs the role of a data-gathering component and provides this data to Tivoli Asset Management for IT. The product collects

- software inventory information
- software use information that will allow you to monitor basic product use and, thanks to Tivoli Common Reporting, observe trends in how certain software assets are used on a daily basis.
- data about hardware in your infrastructure

Together with Tivoli Asset Management for IT Asset Discovery for Distributed allows for full lifecycle asset management. Catalog management is possible thanks to close integration with Software Knowledge Base Toolkit (Launch-in-context tasks)

2. Accurate and easily managed catalog

Customers need a reliable way to validate the discovered inventory. This can be done by combining the catalog (provided by IBM and published regularly with included newer processor technologies), raw inventory and the identified inventory. The validation can take place after the installation of Asset Discovery for Distributed or the initial stages of the upgrade process. The validation should be performed regularly to maximize the probability of accurate software inventory management. The output from the validation process can be exported to Software Knowledge Base Toolkit for updating the knowledge base, which can facilitate the proper generating of an updated catalog.

3. Software use data processor

A new, software use-data processor is provided, which is an improved version of the one that already exists in Tivoli License Compliance Manager Version 2.3. This allows for the support of all relevant IBM pricing and licensing models for distributed platforms and several independent software vendor pricing models as well as detailed information that can be used for custom reporting.

4. License Metric Tool functionalities

Customers can also enjoy the benefits of distributed sub-capacity pricing without installing a separate License Metric Tool infrastructure. All functionalities of License Metric Tool are provided in Asset Discovery for Distributed.

5. Optimized infrastructure

Runtime servers are no longer needed in the Asset Discovery for Distributed infrastructure. The server component can now serve a larger number of agents, up to 45 000. This is possible thanks to the new and optimized code that better handles workloads coming from agents that interact with the server on a regular basis, for example when sending new inventory and use data and downloading catalog or updated agent binaries.

Those who wish to monitor a smaller infrastructure can benefit from the option of installing Asset Discovery for Distributed with the embedded version of WebSphere Application Server, which can be performed quickly with streamlined installation process. A small infrastructure can thus be set up more quickly, which results in costs reduction and the staff having more time available for other system administering tasks.

6. Custom reports

Customers can now generate and view customized reports that can be better tailored to their special needs. To help them enjoy the enhanced reporting functionalities Tivoli Common Reporting is shipped with Asset Discovery for Distributed. Default use reports are provided to facilitate the use of this powerful reporting engine.

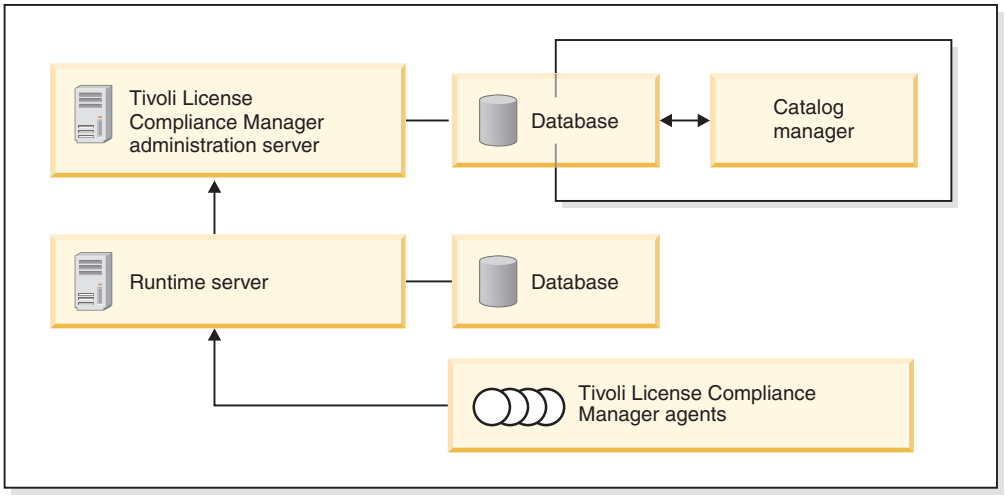
Architectural differences

There are substantial differences between Tivoli License Compliance Manager version 2.3 and Tivoli Asset Discovery for Distributed version 7.2 architectures. The latter product is a part of a bigger family and can be integrated with other products to offer new and enhanced functionalities.

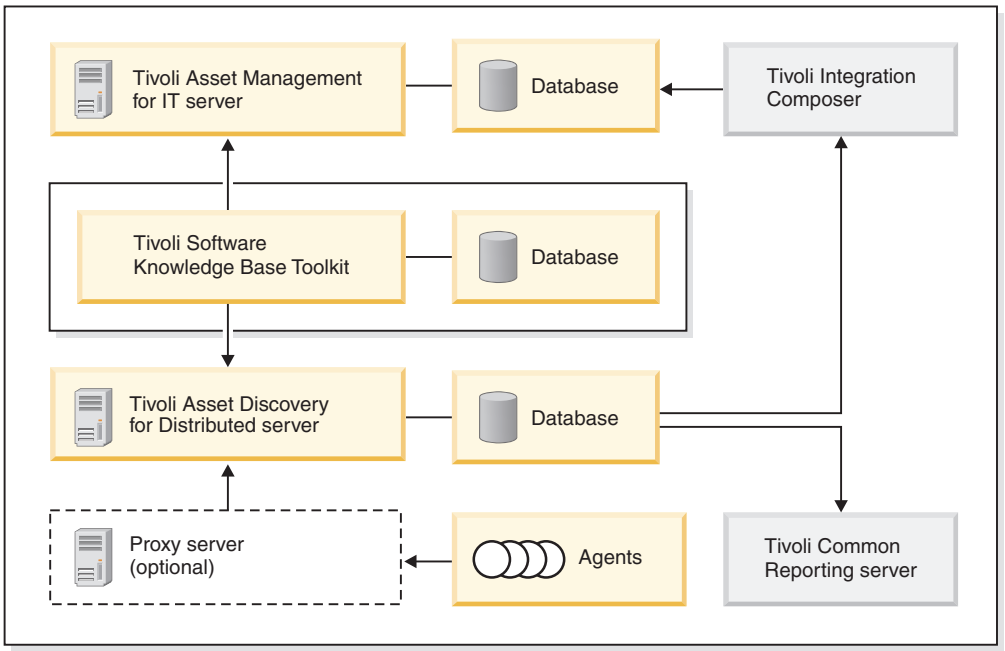
The diagram below depicts Tivoli License Compliance Manager version 2.3 environment before (left side) and after (right side) the upgrade to Asset Discovery for Distributed version 7.2.

Note: Some elements of the infrastructure are installed independently, for example IBM Tivoli Asset Management for IT or IBM Software Knowledge Base Toolkit.

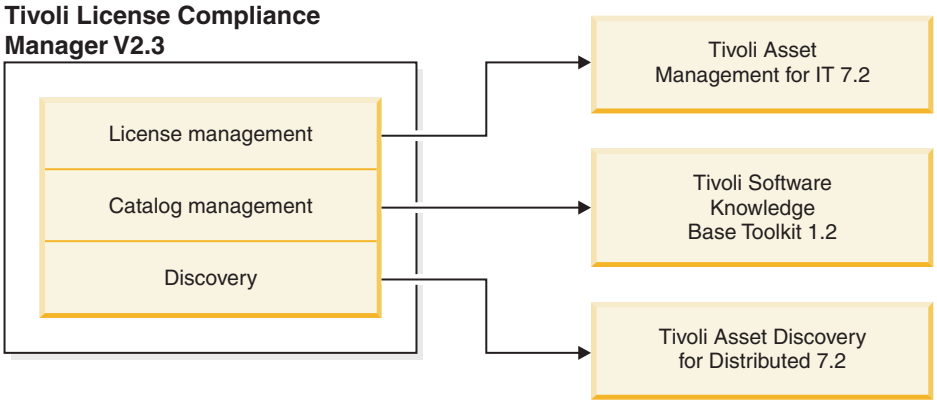
Tivoli License Compliance Manager architecture (before upgrading)



Tivoli Asset Discovery for Distributed in the Asset Management family of products (after upgrading)



This second diagram shows the upgrade from a functional point of view - it shows products in the Asset Management family and the functions implemented in them that they have take over from Tivoli License Compliance Manager.



New infrastructure elements

Tivoli Asset Management for IT

This is the main product in the family. It provides numerous functionalities and benefits, such as

- asset tracking
- asset reconciliation
- contract management
- procurement management
- financial management
- and optionally Service Level Agreement management

It is installed separately from Tivoli Asset Discovery for Distributed server.

Software Knowledge Base Toolkit

This product manages software knowledge information provided by IBM as well as updates made by the customer. It is needed in the early stages of upgrading and migrating from Tivoli License Compliance Manager. Software Knowledge Base Toolkit can be installed on a separate or the same computer as Asset Discovery for Distributed and can be used on a regular basis in managing software catalog.

Proxy servers can be set up in your infrastructure to substitute runtime servers.

Proxy servers replace runtime servers. They can be used temporarily or for extended periods of time, depending on your needs. You can remove them from your infrastructure after the agents have been re-configured. Leave proxy servers if you do not want to change the configuration of version 2.3 agents or if your network topology requires it.

IBM Tivoli Integration Composer adapter

IBM Tivoli Integration Composer adapter is used for integration of data coming from other data sources in the infrastructure, for example for exporting data from Asset Discovery for Distributed to Tivoli Asset Management for IT.

Infrastructure elements that are not upgraded

The following infrastructure elements are absent in the target infrastructure:

Runtime servers

After upgrading and migration of data only the Asset Discovery for Distributed server will store PVU and usage information. Runtime servers

will no longer be used. To route the data from agents to the Asset Discovery for Distributed server you can use one of the several available methods:

1. You can forward data with the use of *proxy servers* that can be installed on the machines which performed the role of runtime servers. Proxy servers are IBM HTTP servers with installed plugins which are able to forward packets to the Asset Discovery for Distributed server. You should set them up if you are not planning to upgrade agents in your infrastructure.
2. You can make appropriate entries in the Domain Name Services server so that former runtime server IP addresses point to the Asset Discovery for Distributed server.

Catalog Manager

Software Knowledge Base Toolkit performs the role of a license signature repository, both for IBM and other vendors' product signatures. Data is exported to Software Knowledge Base Toolkit at the beginning of the upgrade process, updated and imported to Asset Discovery for Distributed server at the end of the upgrade process.

Terminology changes between Tivoli License Compliance Manager and Tivoli Asset Discovery for Distributed

There are a few differences of terms used in both offerings. This section should help you in familiarizing yourself with the new terms that are used in version 7.2 of Tivoli Asset Discovery for Distributed.

Table 24. Terminology changes between Tivoli License Compliance Manager and Tivoli Asset Discovery for Distributed version 7.2

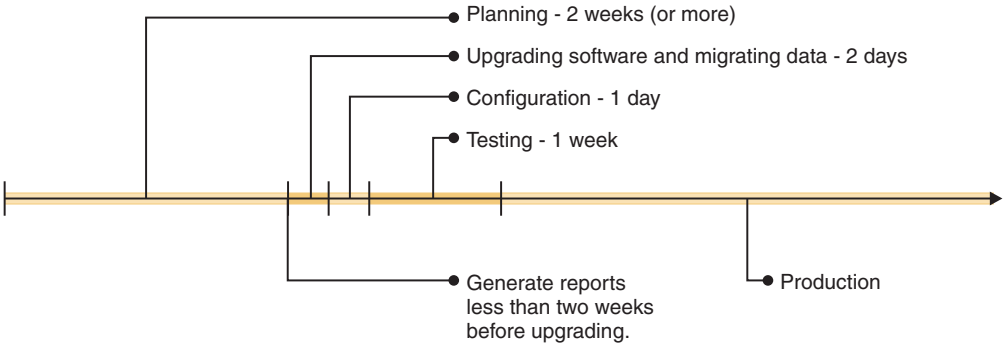
Tivoli License Compliance Manager version 2.3	Tivoli Asset Discovery for Distributed version 7.2
bundle management	product management
division	scan group
organization	(no longer used)
catalog	software catalog
value unit table	PVU table
missing agents	systems without agents

Planning to upgrade from Tivoli License Compliance Manager V2.3 to Tivoli Asset Discovery for Distributed V7.2

Before upgrading from Tivoli License Compliance Manager to Tivoli Asset Discovery for Distributed, you must plan and schedule the activities that are involved. Depending on the size of your monitored infrastructure, the entire process might take two to three weeks, including planning and testing.

As shown in the following drawing, the actual work of upgrading the server software and migrating data can be scheduled to occur during a short service window, for example one or two days. During that time, discovery data is kept in your agents' cache. When the server is back online, the agents will upload the cached data.After the new server is active, you can continue to support License Compliance Manager agents by installing *proxy servers* in place of the runtime servers, or you can change the IP addresses of the hosts defined in a domain name

server (DNS) together with the necessary port numbers so that data is sent directly from V2.3 agents to the Asset Discovery for Distributed server.



1. If you customized your software catalog in License Compliance Manager, for example to create your own signatures, you need to plan to migrate the catalog.
2. Plan your server topology; do server capacity planning.
   a. Read about the architectural changes from License Compliance Manager.
   b. Read the planning topics to determine what other updates you need to install, to meet hardware and software prerequisites.
   c. Decide whether to install on the embedded version of WebSphere Application Server or the one that is bundled with Asset Discovery for Distributed, or on a separately licensed version that you own and which you may need to upgrade. Decide whether to install the Asset Discovery database on a separate computer. These decisions depend on the size of the IT infrastructure that you will monitor.
   d. If you defined multiple *organizations* in License Compliance Manager, plan for their migration to multiple servers.
3. Plan the agent-server communication continuity. In License Compliance Manager agents communicate with the runtime server, not with the administration server. Each agent configuration contains runtime server address and port as parameters. Typically Asset Discovery for Distributed server is placed on a different server than runtime server, so agent's parameters become out-of-date. There are several ways of solving this problem. You can:
   - ensure that Asset Discovery for Distributed server has network address and communication ports previously used by License Compliance Manager runtime server. It can be done by DNS reconfiguration and choosing non-default ports during Asset Discovery for Distributed server installation.
   - use proxy server in place of License Compliance Manager runtime server to forward the data to the Asset Discovery for Distributed server
   - change the configuration of all agents (inconvenient for large environments)
4. Plan the configuration steps that you will take right after upgrading the server. You will need to grant access to designated employees, configure the timing of important administration events, and set up automatic notification.
5. Create test plans. Determine how many computers can be used for testing upgrade and migration activities, and who needs to be involved. Ideally, you should test the communication between agents and the server, aggregation of data, and other functions that support the roles of administrator, software asset manager, and inventory administrator.
6. Determine if you have any agents in your infrastructure that are lower than version 2.3. Take into consideration the fact that if you perform the migration

of data from License Compliance Manager V2.3 to Asset Discovery for Distributed V7.2 those agents will not be able to connect to the upgraded server. Moreover, the database migration process removes all inventory data of those agents from the database. Because of these facts, the upgrade of all the agents to version 2.3 Fix Pack 5 is recommended.

7. If your License Compliance Manager 2.3 environment is Tivoli Configuration Manager-integrated, you need to disintegrate it before upgrading to Asset Discovery for Distributed.
8. Finally, schedule the server upgrade and data migration to occur *two weeks or less* after the end date of the period covered by the last IBM use report generated in License Compliance Manager. This is because of the fact that in Asset Discovery for Distributed a maximum of two weeks before database migration can be recalculated. Therefore, to maintain continuity of reporting, the time delay between running IBM Use report and migrating the database must be less than two weeks.

Planning and sizing checklist for upgrading from Tivoli License Compliance Manager Version 2.3

The checklist should help you plan the process of upgrading your Tivoli License Compliance Manager V. 2.3. to Tivoli Asset Discovery for Distributed V. 7.2. Use the checklist to carefully control the planned upgrade and migration steps.

Table 25. Upgrade planning and sizing checklist

Number	Step	Time (hours)	Date	Comments
Planning phase				
1	**Define Upgrade Phases**			
1.1	Define Test Upgrade			
1.2	Define Production Upgrade			
2	**Define resources:**			
2.1	Define Personnel			
2.2	Define Hardware			
3	**Plan the export of data**			
3.1	Plan migration of data into Tivoli Asset Management for IT and Software Knowledge Base Toolkit			
Testing Phase (Proof-of-concept upgrading of the server, test upgrading of selected agents)				
4	**Server Upgrade - Testing Phase**			
4.1	System verification: hardware, patches for OSs, file system space requirements			
4.2	Generate your last IBM report as close as possible to the date of upgrade			
4.3	Export the contents of the catalog to Software Knowledge Base Toolkit			
4.4	Disconnect agents from the runtime servers, upload data to the administration server and remove the runtime servers			
4.5	Backup and upgrade the database			
4.6	Migrate the data			

Table 25. Upgrade planning and sizing checklist (continued)

Number	Step	Time (hours)	Date	Comments
4.7	Install the server (on the embedded or Base WebSphere Application Server)			
4.8	Set up proxy servers (data forwarding)			
4.9	Verify agent-to-server communication			
4.10	Import data from Software Knowledge Base Toolkit			
4.11	Verify the completeness of migrated and imported data			
5	**Agent Upgrade - Testing Phase**			
5.1	Define target agents			
5.2	Execute the upgrade of Target Agents			
5.3	Validate the upgrade of Target Agents			
Production Phase (Upgrading the software on target servers and computers after successfully testing)				
6	**Server Upgrade - Production Phase**			
6.1	System verification: hardware, patches for OSs, file system size requirements			
6.2	Generate your last IBM report as close as possible to the date of upgrade			
6.3	Export the contents of the catalog to Software Knowledge Base Toolkit			
6.4	Disconnect agents from the runtime servers, upload data to the administration server and remove the runtime servers			
6.5	Backup and upgrade the database			
6.6	Backup the database			
6.7	Migrate the data			
6.8	Install the server (on the embedded or Base WebSphere Application Server)			
6.9	Set up proxy servers (data forwarding)			
6.10	Verify agent-to-server communication			
6.11	Import data fromSoftware Knowledge Base Toolkit			
6.12	Verify the completeness of migrated and imported data			
7	**Agent Upgrade - Production Phase**			
7.1	Define target agents			
7.2	Execute the upgrade of Target Agents			
7.3	Validate the upgrade of Target Agents			
8.	**Post-upgrade steps**			
8.1	Remove the data forwarding solution (e.g. proxy servers)			
9	**Configure the Tivoli Asset Discovery for Distributed server**			

Table 25. Upgrade planning and sizing checklist (continued)

Number	Step	Time (hours)	Date	Comments
9.1	Configure user accounts and notifications			
9.2	Import Processor Value Unit table from IBM web site			
9.3	Verify the completeness of the new User Interface (Integrated Solutions Console)			
10	**Post-launch support**			
10.1	Project Management			
10.2	Education for day-to-day maintenance			
10.3	Contingency (for unknown or unexpected issues)			
	Estimated total project hours:			

Preparing to upgrade from Tivoli License Compliance Manager to Tivoli Asset Discovery for Distributed 7.2

Before upgrading your product, you need to review all of the applicable upgrade prerequisites and pre-upgrade tasks to ensure that the upgrade proceeds smoothly.

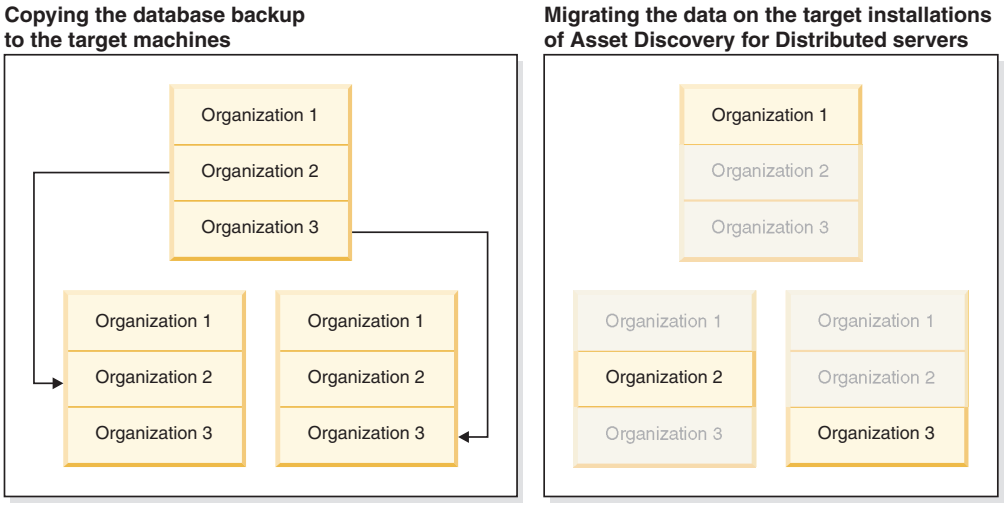
1. Plan the entire upgrade process. This might take from one to three weeks.
2. Install software prerequisites:
   a. Install Software Knowledge Base Toolkit.
   b. If you plan to install on a separate, stand-alone version of WebSphere Application Server instead of on the one that is embedded with Asset Discovery for Distributed, ensure that you have Version 6.1, Fix Pack 23. To confirm, run the **versionInfo** command. For more information see http://publib.boulder.ibm.com/infocenter/wasinfo/v6r0/index.jsp?topic=/com.ibm.websphere.nd.doc/info/ae/ae/rins_versionInfo.html
   c. Confirm that you have DB2 version 9.1 or higher on the Asset Discovery for Distributed server. If you have an older version, upgrade it. For more information see http://publib.boulder.ibm.com/infocenter/db2luw/v9/index.jsp.
   d. For other prerequisites, including operating systems and required fix levels, refer to the installation guide for Asset Discovery for Distributed.
3. Generate IBM Use report as close to the database migration date as possible if you want the remaining data to be migrated and recalculated according to the new pricing rule. Keep in mind that in Asset Discovery for Distributed V7.2 only two weeks before migration date is recalculated. Generating the reports at the recommended time maintains the continuity of reporting in the upgraded product. See http://publib.boulder.ibm.com/infocenter/tivihelp/v3r1/index.jsp?topic=/com.ibm.itlm.doc_2.3/admin/ibmusage.html.
4. (Recommended) Back up your database so you can recover it in case an error occurs during the upgrade process. For more information see http://publib.boulder.ibm.com/infocenter/db2luw/v9/index.jsp.
5. (Recommended) Back up the keystores on the Tivoli License Compliance Manager runtime server (servers). You will need them later on when you will be configuring secure connection between the agents and the Asset Discovery for Distributed server. This step is only needed if secure communication is enabled in Tivoli License Compliance Manager.

Migrating multiple organizations from Tivoli License Compliance Manager

Tivoli License Compliance Manager supported the creation of different organizations on a single administration server, so large enterprises could define different monitoring structures and segregate the licenses and reports that different administrators worked with. If you defined multiple organizations in License Compliance Manager, you must now migrate each organization to a separate instance of Tivoli Asset Discovery for Distributed.

You must choose one organization, at a time, when you migrate data from Tivoli License Compliance Manager to Tivoli Asset Discovery for Distributed server. If you plan to migrate the data of the other organizations, you must install as many instances of the Tivoli Asset Discovery for Distributed server as there are organizations in the Tivoli License Compliance Manager database. So if, for example, you had three *organizations* defined on your old server for Company A, Company B, and Company C, now you need three servers, three application servers and three databases on which you will install three instances of Tivoli Asset Discovery for Distributed.

Each database must be separately backed up and restored on the target server. The machine used previously for administration server can be reused for the new (version 7.2) instance of the server. This case is illustrated in the diagram below.



You must remember to perform the necessary steps in the appropriate order. The following is the summary of steps:

1. Procure the servers
2. Install operating systems and necessary patches or updates
3. Install the software prerequisites
4. Run the backup of the of the administration server database
5. Copy the backup files to the target servers
6. Run the database restores multiple times (once on each of the target servers)
7. Run the Tivoli Asset Discovery for Distributed installation program multiple times, each time choosing the appropriate organization to migrate only given subset of data

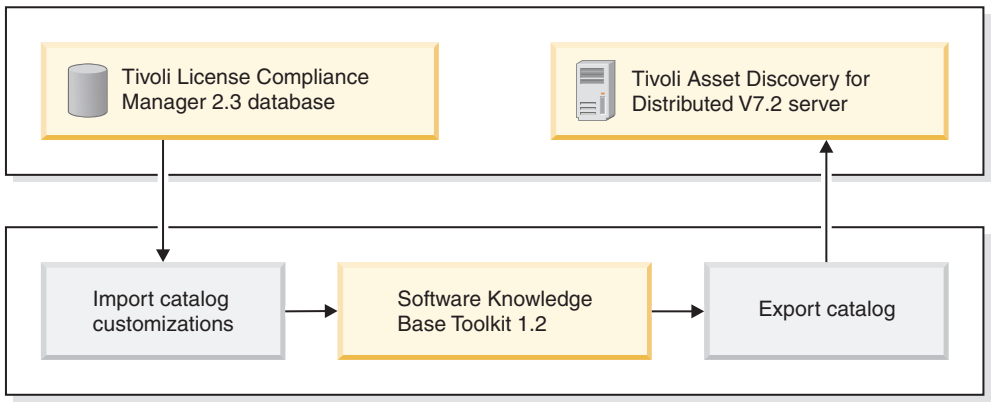
The backup or restore procedures require that the same operating system is installed on the source and target machines. DB2 backup and restore functions have some operating system-related limitations. For more information, see DB2 information center.

Migrating customized data from the IBM Tivoli License Compliance Manager database

Whether you customized the catalog in Tivoli License Compliance Manager or not, for example to create or modify software signatures, you should migrate the catalog to the new environment. It is a mandatory step in the process of upgrading from Tivoli License Compliance ManagerV2.3 to Tivoli Asset Discovery for Distributed.

In Tivoli Asset Discovery for Distributed you will use the new Software Knowledge Base Toolkit feature to add and change signatures in the knowledge base, and export catalogs from there. Similarly, to migrate your old catalog from License Compliance Manager, you must first import your customized data into the knowledge base and then export it as a catalog that you can use with Asset Discovery.

The following diagram presents a high level overview of the migration process and all its stages.



Migrating the data from License Compliance Manager database into the Software Knowledge Base Toolkit database involves the following steps:

1. Setting the parameters in "The migration.properties file" on page 52.
2. "Converting customized data to the XML catalog format."
3. "Importing customized data into the knowledge base" on page 53
4. "Exporting the migrated catalog entries" on page 54

Converting customized data to the XML catalog format

When migrating your old catalog to Tivoli Asset Discovery for Distributed, the first step is to convert your existing data into a format that can be imported into Software Knowledge Base Toolkit.

Later, you will export from the knowledge base to your new catalog.

Before you begin

You must have Software Knowledge Base Toolkit installed before starting the task.

To do this:

1. Find the `migration.properties` file that is located in the `KBCMS\bin` catalog in the directory where you install Software Knowledge Base Toolkit.
2. In the `migration.properties` file provide credentials for accessing the Tivoli License Compliance Manager database and the name of the output file that will be generated in the canonical XML format.
3. In the `KBCMS\bin` catalog in the directory where Software Knowledge Base Toolkit is installed, run one of the following files:
   - On Windows operating systems: `migrate.bat`
   - On other operating systems: `migrate.sh`
4. Verify if the customization tool generated a canonical XML document. It should be located in the `KBCMS\bin` directory.

   Note: The XML file and the log file are stored in the same directory. Both files have the names that you specified in the properties file.

The migration.properties file:

The migration.properties file provides information about the Tivoli License Compliance Manager database, the user credentials that are needed to access it, and the properties of the canonical XML file that is generated by the customization tool.

The file is located in the `KBCMS\bin` catalog in the directory where you install IBM Tivoli Software Knowledge Base Toolkit. The default location of the file for Windows is `C:\Program Files\IBM\SoftwareKnowledgeBaseToolkit\KBCMS\bin`.

Source properties

host = *IP_address*
Specifies the IP address or the host name of the server or computer on which the Tivoli License Compliance Manager database is installed.

port = *port_number*
Specifies the port number on which the Tivoli License Compliance Manager database can be accessed. The default value is *50000*.

db_name = *database_name*
Specifies the name of the Tivoli License Compliance Manager database that you want to access. The default value is *TLMA*.

username = *user_ID*
Specifies the ID of the user to access the Tivoli License Compliance Manager database.

password = *user_password*
Specifies the password for the user account just specified.

Output properties

This section describes the properties of the output file that will be generated by the tool.

filename_output = *file_name*
Specifies the name of the XML file generated by the conversion tool. You will need to provide the file name and path later, when you import this file into the software knowledge base.

Log properties

This section describes the properties of the log file that will be generated by the tool.

log_filename = *file_name*
Specifies the name of the log file.

log_level = *SEVERE* | *WARNING* | *INFO* | *CONFIG* | *FINE* | *FINER* | *FINEST*
Specifies the level of detail that you want the log file to contain. The default value is CONFIG, which is recommended.

Importing customized data into the knowledge base

After running the customization tool that converts your Tivoli License Compliance Manager data into the XML format, the next step is to import the output from the tool into Software Knowledge Base Toolkit.

When the canonical XML document is imported, its content is analyzed for conflicts with the data that is currently stored in your knowledge base. If such conflicts are detected, you can view then to learn about the reasons.

To import the output of the customization tool into the knowledge base, follow the steps provided.

Note: You need to be an inventory administrator or an asset manager to perform the task.

1. Log on to Software Knowledge Base Toolkit.
2. Upload the XML file to software knowledge base.
   a. To do this, select **Manage Imports → Canonical XML Document**, and click **New Import**.
      - (Optional) Specify a descriptive name for the new import task, for example: `TLCM migration`.
   b. Click **Browse** to locate the output file that you created when you converted your old catalog. You defined the file in the migration.properties file. Click **Open**.
   c. Provide a reason for introducing changes to the knowledge base, for example `Migrating catalog changes from Tivoli License Compliance Manager`.
   d. Click **OK** to start processing the file.

      Note: If the knowledge base has been modified by means of Catalog Manager, it is not recommended to use the **Overwrite knowledge base data** option because it might break the import.
   e. Click **Refresh** to check the processing results. If the file has been processed successfully, the status will be `Completed`.
3. View the list of conflicts which were found between the import file and the data stored in the knowledge base.

   Note: The data for which no conflicts are detected will be imported into the knowledge base.

a. Open the task marked with the **conflicting** icon  .
b. View the Conflict Areas table for the data area that have been detected as conflicting with knowledge base content. For more information on the conflict types, see the Software Knowledge Base Toolkit information center.

All data for which no conflicts were found is now added to the software knowledge base. The date of the document import is recorded as the date of the last modification of the existing knowledge base entries. To view a detailed report containing information on all the manufacturer, software, and signature entries that were created or modified during the import of a selected document, see **Manage Imports → Import Summaries**. The **Import Summaries** panel contains also information about failures, and should be checked to verify if and what type of failures have happened.

Exporting the migrated catalog entries

After importing your old catalog data to the software knowledge base, the next step in migrating your old catalog is to export that content from the knowledge base to the IBM Tivoli Asset Discovery for Distributed catalog.

1. From the Software Knowledge Base navigation bar, select **Manage Knowledge Base Exports → Export Catalogs**.
2. In the New Export Task section of the window, select **IBM Tivoli Asset Discovery for Distributed** and click **Launch**. A new task is added to the Export Tasks table. You can use this table to manage your export task and to monitor its progress.
3. When the export task has finished, you can see the  icon, click **Refresh** in the Exported Knowledge Base Content section which shows a tree representation of all the catalogs that you export. They are grouped according to the export type.
4. In the Published Knowledge Base Content section, click the  icon to open the folder containing the IBM Tivoli Asset Discovery for Distributed catalog that you exported.
5. Click the context menu icon  next to the catalog file and then click **Download** to download the file.

You can now import the catalog containing customized data migrated from the database into the application so that the complete software catalog data can be distributed to the agents.

Uninstalling Tivoli License Compliance Manager

Before installing Tivoli Asset Discovery for Distributed, the next upgrade step is to uninstall License Compliance Manager administration and runtime servers, leaving only the old administration server database.

To uninstall the administration and runtime servers, perform the following tasks:

1. Disconnect agents from the runtime servers in your infrastructure so that data is no longer sent to the administration server.
2. Uninstall the runtime servers.
3. Uninstall the administration server.

Disconnecting agents from runtime servers

You need to disconnect Tivoli License Compliance Manager agents so they no longer send data to the old administration server. Runtime servers are absent in the Tivoli Asset Discovery for Distributed version 7.2 topology; you can optionally replace them with proxy servers if you do not plan to change the configuration of the agents right away (server IP address and port number).

If you have more than one runtime server, you need to repeat this process for each runtime server in your old environment.

Before you begin

You will require the user ID and password of Super Administrator. Prepare the list of your runtime servers and their IP addresses (if you have more than one).

Disconnected agents store data in their cache during the upgrade process. The data is limited to the hardware inventory and usage data information. For software inventory, only the last scan execution result are stored.

To block the connection between agents and the given runtime server perform the following steps:

1. Open the Integrated Solutions Console of each runtime server in your browser by specifying its IP address and port:
   - (if secure connection is not enabled) `http://<RUNTIME_SERVER_IP_ADDRESS>:9060/ibm/console/`

     This port value is default for insecure connections. However, different port numbers can be used.
   - (if secure connection is enabled) `https://<RUNTIME_SERVER_IP_ADDRESS>:9043/ibm/console/`

     This port value is default for secure connections. However, different port numbers can be used.
2. Log on to the Integrated Solutions Console User Interface using your **Administrator** credentials.
3. Click **Servers** → **Application servers** → **IBM TLCM runtime server**.
4. In the **Container Settings** section, expand **Web Container Settings** and click **Web container transport chains**.
5. In the Application servers pane, in the list of Web container transport chains, select the **WCInboundDefault** check box. The Configuration tab opens.
6. In the General properties area, clear the **Enabled** check box. Click **Apply**, then click **OK** to close the Configuration tab.

   Note: The same steps must be performed for **WCInboundDefaultSecure** in case secure agent-to-runtime communication is enabled.
7. After you have made all the necessary changes in the Integrated Solutions Console, click the **Save** link. You can now log out of the Integrated Solutions Console.
8. To verify if agents are disconnected from one of the runtime servers, restart the server and log on to the agent computer that was previously connected to the runtime server and issue the **tlmagent -p** command. If the command fails, it means that the agent-runtime server communication has been disabled.

Now, you can upload the data collected in runtime server database to the License Compliance Manager administration server and uninstall the runtime server. Repeat the procedure for other runtime servers in your infrastructure.

Uninstalling the runtime servers

After disconnecting Tivoli License Compliance Manager agents, the next tasks in migrating to Tivoli Asset Discovery to Distributed are to upload data from each runtime server to the administration server, and then uninstall the runtime servers and their databases. Later, you will migrate the uploaded data from the administration server to Asset Discovery for Distributed.

Before you begin

- You must have the following operating system privileges:
  - Windows Administrator
  - UNIX root
- (Recommended) Back up the runtime server database before you uninstall the server.

Runtime servers do not exist in Tivoli Asset Discovery for Distributed infrastructure and their uninstallation is the next step in the upgrade procedure. As part of migration from Tivoli License Compliance Manager, you will move data that is currently stored on runtime servers by reconfiguring them to transmit their data to the administration server within an hour, restarting the runtime servers and waiting long enough for data transmission to occur, and then uninstalling the runtime servers.

Important:
Perform the following steps on every runtime server in your License Compliance Manager environment.

1. Stop the runtime server by issuing the tlmcli -c srvstop command from a command line.

   The command line interface files are located in the following directories:

   - Windows `C:\Program Files\IBM\TLM\runtime\cli\tlmcli`
   - UNIX `/opt/IBM/TLM/runtime/cli/tlmcli`

   The server might take up to 20 minutes to stop, depending on the capacity of the machine and amount of data in the database.
2. Edit the `System.properties` file by assigning the value of **adminUploadPeriod** parameter to **60** (the lowest value). The `System.properties` file is located in the following directory:

   - Windows `C:\<RUNTIME_SERVER_INSTALLATION_DIRECTORY>\runtime\SLM_Runtime_Application.ear\slm_runtime.war\WEB-INF\conf`
   - UNIX `<RUNTIME_SERVER_INSTALLATION_DIRECTORY>/runtime/SLM_Runtime_Application.ear/slm_runtime.war/WEB-INF/conf`
3. Enter the command line interface directory on the runtime server computer and start the server by issuing the tlmcli -c srvstart command.
4. Wait at least one hour for the runtime server to send its most recent data to the administration server.
5. Stop the runtime server again, as described in step 1. Now, after the data has been uploaded, you can uninstall the runtime server and its database.

6. Start the uninstallation wizard. (If you prefer to uninstall runtime servers in silent mode, refer to the instructions given below.
   - Windows
     a. Select the **Add/Remove Programs** option from the **Control Panel**. Select **Tivoli License Compliance Manager** and click **Change/Remove**. When the installation wizard opens, click **Next**.
     b. On the new page, select *both* the runtime server and the runtime server database for uninstallation and click **Next**.
     c. On the next page, select the option for dropping database and click **Next**. If you are operating WebSphere Application Server in a secure cell, a panel is displayed for you to enter the User ID and Password to access the WebSphere Application Server secure cell. Click Next to continue the uninstallation.
     d. Reboot the computer.
   - UNIX Navigate to the directory `<INSTALL_DIR>\_uninst` and run the `uninstaller.bin` file.

   The wizard will begin detecting the Tivoli License Compliance Manager elements present on your computer. The uninstall features window is displayed.
7. Select the option to uninstall the License Compliance Manager database, then click **Next**. The wizard displays a panel showing the features to be uninstalled.
8. Click **Next** to commence the uninstallation.
9. If you have selected to uninstall a server, and you are operating WebSphere Application Server in a secure cell, a panel is displayed for you to enter the User ID and Password to access the WebSphere Application Server secure cell. Click **Next** to continue the uninstallation.
10. Click **Finish** when the uninstallation is complete to exit from the wizard.

Uninstalling runtime servers in silent mode:

As an alternative to uninstalling from a wizard, you can run a script from the command line.

1. Navigate to the directory `<INSTALL_DIR>\_uninst` and open the `ITLM_23_serversUninstall_response.txt` response file in a text editor. This file defines arguments to set each parameter that must be provided to the Tivoli License Compliance Manager uninstall wizard.
2. Change the value of the following parameters to `true`:
   - **-P runtime.activeForUninstall=true**
   - **-P runtimeDB.activeForUninstall=true** (This parameter specifies whether or not the runtime server database should be uninstalled).
   - **-W uninstallFeature.dbDropping=true**

   Both components need to be uninstalled: the runtime server and the runtime server database.
3. Launch the uninstall command with the following arguments:
   ```
   uninstaller.bin -silent -options ITLM_23_serversUninstall_response.txt
   ```
4. Restart the machine.

Now that you have uploaded data from the runtime servers and uninstalled them, the next step is to shut down the Tivoli License Compliance Manager administration server.

Uninstalling the administration server

After uninstalling the runtime servers, the next stage in migration from Tivoli License Compliance Manager is uninstalling the administration server. You will not uninstall the administration database though, because you need to migrate its contents later.

Before you begin

- You must have the following operating system privileges:
  - Windows Administrator
  - UNIX root
- You will need to know the user ID and password of a DB2 administrator ID with sysadm, syscontrol, or sysmaint privileges.
- If you run the administration server on IBM WebSphere Application Server in a secure cell, you will require the user ID and password to access the secure cell.
- (Recommended) Back up theadministration server database before you uninstall the server.

To do this:

1. On the administration server, navigate to the command line interface directory and run the tlmcli -c srvstop:
   - Windows `C:\Program Files\IBM\TLM\admin\cli\tlmcli -c srvstop`
   - UNIX `/opt/IBM/TLM/admin/cli/tlmcli -c srvstop`

   The server stops.
2. Back up the Tivoli License Compliance Manager database. Log on to DB2 with the user ID of the DB2 instance owner.
3. Start the DB2 Command Line Processor.
   - Windows db2cmd
4. Create a directory where you will back up the database by issuing the **mkdir** command:

   ```
   mkdir /backup_directory
   ```
5. Issue the backup command:

   ```
   db2 backup database db_name to backup_directory
   ```

   where *db_name* is the name of the database, and *backup_directory* is the full path to where you want to back up the database. You will receive a message indicating that the backup was successful.
6. You can now uninstall the administration server. To uninstall the server in interactive mode select the **Add/Remove Programs** option from the **Control Panel**. Highlight **Tivoli License Compliance Manager** and click **Change/Remove**. The wizard will begin detecting the Tivoli License Compliance Manager elements present on your computer. The uninstall features window is displayed.
7. Deselect the option to uninstall the Tivoli License Compliance Manager database, then click **Next**. The wizard displays a panel showing the features to be uninstalled.
8. Click **Next** to commence the uninstallation.

9. If you have selected to uninstall a server, and you are operating WebSphere Application Server in a secure cell, a panel is displayed for you to enter the User ID and Password to access the WebSphere Application Server secure cell. Click **Next** to continue the uninstallation.
10. Click **Finish** when the uninstallation is complete to exit from the wizard.

Uninstalling administration server in silent mode:

As an alternative to uninstalling from a wizard, you can run a script from the command line.

1. Navigate to the directory `<INSTALL_DIR>\_uninst` and open the `ITLM_23_serversUninstall_response.txt` response file in a text editor. This file defines arguments to set each parameter that must be provided to the Tivoli License Compliance Manager uninstall wizard.
2. Change the value of the **-P adminDB.activeForUninstall=** parameter to `false`. This parameter specifies whether or not the administration server database should be uninstalled.

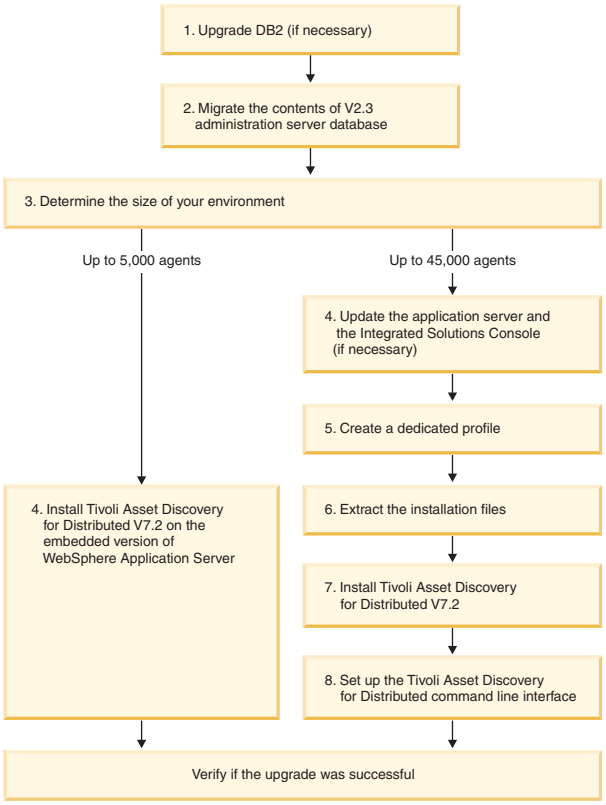
   ```
   -P adminDB.activeForUninstall=false
   ```

3. Launch the uninstall command with the following arguments:

   ```
   uninstaller.bin -silent -options ITLM_23_serversUninstall_response.txt
   ```

Installing the server and migrating the database

Having uninstalled the License Compliance Manager server, you will migrate the administration server database and install the Asset Discovery for Distributed server. The path that you take depends on the size of your environment. This will also affect your decision whether to install DB2 on a separate or the same computer as Asset Discovery for Distributed.



To install your server perform the following steps:

1. Upgrade DB2 if you have version lower that 9.1.
2. Use the installation wizard to migrate the contents of the Tivoli License Compliance Manager administration server database to the Asset Discovery for Distributed 7.2 database.
3. Determine the size of your environment and follow the appropriate path:
   - **Up to 5000 agents**: install on the embedded version of WebSphere Application server.
   - **Up to 45000 agents**: install on the standalone, separately licensed version of WebSphere Application server.
4. If you have decided to manage a smaller infrastructure install Asset Discovery for Distributed using interactive installer or install in silent mode. If you are going to manage a large infrastructure, determine the version of your WebSphere Application Server. If it is lower than V6.1, upgrade it. Verify that WebSphere Application Server fix pack 6.1.0.23 and Integrated Solutions Console update version 7.1.0.7 are installed. If not, update them.
5. Create a dedicated profile for Asset Discovery for Distributed.
6. Extract the installation files by running interactive installer. The extracted files are necessary in the installation of the server and in setting up the server command line interface.
7. Install the server on the separately licensed (Base) version of WebSphere Application Server. The server can be installed on a different machine than the database. You can use sample scripts or you can install the application manually.
8. Set up the Asset Discovery for Distributed command line interface.

Finally, verify if the upgrade has been successful.

Upgrading DB2

Ensure that the DB2 you are going to use in the upgrade process meets the Tivoli Asset Discovery for Distributed Version 7.2 requirements. If the version is lower, upgrade it to Version 9.1 or 9.5.

The DB2 software is not upgraded automatically, either when upgrading on the embedded or base version of WebSphere Application Server. For information how to upgrade DB2 to the target version refer to the highest level topics in DB2 information centers:

- Migration to DB2 Version 9
- Migration to DB2 Version 9.5

Migrating the contents of the Tivoli License Compliance Manager administration server database

Migrate the contents of the Tivoli License Compliance Manager administration database which contains definition of divisions, agent configurations, inventory data and the definition of the infrastructure topology. Moreover, the database design has changed since License Compliance Manager.

Before you begin

- You must have the following operating system privileges:
  - Windows Administrator
  - UNIX root
- You require a valid DB2 administrator ID.
- Do all tasks outlined in *Planning the upgrade,* and *Preparing to upgrade*. These include backing up the administration database, running a final set of reports in your old environment, and installing the required level of IBM DB2 software.

Note:

- If you are migrating the data of another organization (in Asset Discovery for Distributed V. 7.2 organization is called "customer") and you have multiple organizations defined in Tivoli License Compliance Manager, you need to restore database from the backup on the machine where you have the new database component installed.
- If you have any agents in your infrastructure that are lower than version 2.3 and if you perform the migration of data from License Compliance Manager V2.3 to Asset Discovery for Distributed V7.2 those agents will not be able to connect to the upgraded server. What is more, the database migration process removes all inventory data of those agents from the database. Because of these facts, the upgrade of all the agents to version 2.3 Fix Pack 5 is recommended.

When upgrading on the embedded or standalone WebSphere Application Server, you need to migrate the contents of the Tivoli License Compliance Manager database to the Tivoli Asset Discovery for Distributed database format before deploying Tivoli Asset Discovery for Distributed V7.2. These functions are performed using the launchpad.

To do this:

1. Start the Tivoli Asset Discovery for Distributed launchpad from the root directory of the product disk or the downloaded installation image by starting:
   - UNIX launchpad.sh
   - Windows launchpad.exe
2. Launch the installation wizard by clicking **Install** and **Install database components**.
3. The welcome screen appears and shows that Administration server database has been detected by the installer. The installation wizard detects the existing administration database and confirms that it will be migrated to 7.2.0.0. Click **Next**.
4. Read through the license agreement and accept the terms. Click **Next**.
5. Provide the password for the existing **tlmsrv** user. Click **Next**.
6. If more than one customer is defined in the database, select the one you want to migrate and the scan group you want to make default. ATivoli Asset Discovery for Distributed instance only supports one customer. If you want to migrate the data of the other organizations, you must perform the migration procedure as many times on separate machines as there are organizations in the Tivoli License Compliance Manager database. Click **Next**.
7. Select the security options that you chose during planning. If you set the minimum or medium security level, agents can communicate with the Asset Discovery for Distributed server by either the secure or the unsecure port, depending on the security level defined when the agent was deployed. If you

set the maximum security level, when you deploy agents you must set the same level of security for all agents that are to contact the Asset Discovery for Distributed server.

8. Check the information about the migration and ensure that you have enough space to complete it, then click **Next** to start migrating data.
9. When the migration completes successfully, a summary panel opens showing the migration tasks that were completed.

When this procedure has been completed successfully, you will have migrated the contents of the License Compliance Manager V. 2.3 database to the new - Asset Discovery for Distributed V. 7.2 one.

Now you can begin the installation of Asset Discovery for Distributed.

Installing Tivoli Asset Discovery for Distributed 7.2 on the embedded version of the IBM WebSphere Application server

Asset Discovery for Distributed includes an embedded version of IBM WebSphere Application Server that you can use for the administration server if you plan to support fewer than 4500 agents.

The installation wizard installs the Tivoli Asset Discovery for Distributed server on a computer where the DB2 database has already been upgraded and the data has been migrated from Tivoli License Compliance Manager.

Before you begin

Do not start the installation until you meet the following prerequisites:

- Do all tasks outlined in *Planning the installation*, including capacity planning and security planning.
- Do all tasks outlined in *Planning the upgrade*, and *Preparing to upgrade*. These include backing up the administration database, running a final set of reports in your old environment, and installing the required level of IBM DB2 software.
- You must have the following operating system privileges:
  - Linux UNIX root
  - Windows Administrator
- You require the password for the existing tlmsrv user. The tlmsrv user is used for communications between the Tivoli License Compliance Manager server and its DB2 database. The user ID tlmsrv was created on the computer where DB2 was installed and was assigned the password. If it does not exist, the user tlmsrv is created during upgrade.

You can install the server from the installation launchpad.

To do this:

1. Start the Tivoli Asset Discovery for Distributed launchpad from the root directory of the product disk or the downloaded installation image by entering:
   - Linux UNIX `launchpad.sh`
   - Windows `launchpad.exe`
2. Launch the installation wizard by clicking **Install** and **Install server and database components**.
3. Answer the installation wizard questions as follows:

a. After accepting the license agreement, choose **Production Environment** as the installation type. Click **Next**.
b. After specifying the target installation directory, advance to the next page and select **Administration server** as the component that you want to install. Click **Next**.
c. Select **Install the server on the embedded version of WebSphere Application server** and then **Browse** to select the destination installation directory. Click **Next**.
d. Specify the ports to be used in server and agent communications or use the default ones. Click **Next**.
e. Connect to the administration server database by entering the password for the existing **tlmsrv** user. If it is in a distributed environment, then the **tlmsrv** exists on the remote server computer. Provide the port number which will be used by the server software for connecting to the database. You can use the **Test Connection** button to test the connection with the database. Click **Next**.
f. If more than one organization (in version 7.2 organization is called "customer") is defined in the database, select the one you want to migrate and the scan group you want to make default. Click **Next**. Unlike Tivoli License Compliance Manager, a Tivoli Asset Discovery for Distributed instance only supports one customer. If you have multiple customers, you need to install one server for each.

4. Click **Next**. Check the information about the installation process and ensure that you have enough space to complete the installation, then click **Next** to start installing. When the installation process completes successfully, a summary panel opens showing the tasks that were completed.
5. To verify that the installation was successful, log into the Integrated Solutions Console and check if Tivoli Asset Discovery for Distributed appears in the navigation bar.

You have upgraded the Tivoli License Compliance Manager 2.3 server components to Tivoli Asset Discovery for Distributed 7.2 on the embedded version of WebSphere Application Server.

If you do not plan to re-configure your License Compliance Manager agents right away, proceed to *Configuring the IBM HTTP server to forward agent data traffic on the embedded WebSphere Application Server* . Forwarding of data is necessary if the runtime server was installed on a different machine than the administration server or there were multiple runtime servers in your infrastructure.

Installing Tivoli Asset Discovery for Distributed on a stand-alone version of WebSphere Application server

If you plan to support more than 5000 agents, you need to install the Tivoli Asset Discovery for Distributed server on a stand-alone version of IBM WebSphere Application Server.

Before you begin

Do not start the server installation unless you meet the following prerequisite:

- You must have version 6.1 of WebSphere Application Server with fix pack 23 and Integrated Solutions Console version 7.1.0.7. up and running on the computer that will perform the role of Asset Discovery for Distributed server.

- It is advisable to create a separate profile for the installation of Tivoli Asset Discovery for Distributed on top of base WebSphere Application Server. This will prevent application conflicts and the use of the same binaries by two different applications.

Upgrading to Asset Discovery for Distributed involves the following steps. You will do some steps from the installation wizard, and other steps by preparing scripts and running them from a command-line prompt.

To install Tivoli Asset Discovery for Distributed perform these steps:

1. Update the WebSphere Application Server with the latest Fix Pack and the Integrated Solutions Console update.
2. Create a dedicated profile.
3. Extract the installation files that you will need to run the installation scripts.
4. Edit the SetupWAS.properties file.
5. Install the server components You may want to install the server components manually.
6. Enable the Asset Discovering for Distributed command-line interface.

Updating WebSphere Application Server and Integrated Solutions Console:

After installing WebSphere Application Server and Integrated Solutions Console, you need to update them with the latest fix packs.

Before you begin

If you are reusing the existing installation of WebSphere Application Server, verify its version using the versionInfo command.

1. Download the Update Installer from the following Web site: http://www-01.ibm.com/support/docview.wss?rs=180&uid=swg24020212 . If you have an earlier version of Update Installer on your computer, you need to uninstall it before installing this one.
2. Stop WebSphere Application Server.
3. Download the fix pack 23 for WebSphere Application Server 6.1 from: http://www-01.ibm.com/support/docview.wss?rs=180&uid=swg24022250.
4. Copy the Integrated Solutions Console update file from the `DIR_WHERE_THE_DVD_IS_MOUNTED/server/fixpacks/ISC/6.1.0.11-WS-WASFeature-FEISCAE7107.pak` to the same folder where you downloaded the fix pack 23 for WebSphere Application Server.
5. Run the Update Installer installation file.
6. On the Welcome panel, read what products are supported and click **Next**.
7. Specify the path to the WebSphere installation directory, for example `C:\Program Files\IBM\WebSphere\AppServer on Windows systems` (Windows) or `/opt/IBM/WebSphere/AppServer` (UNIX).
8. Select **Install maintenance package**.
9. Enter the name of the directory where you had placed the update and fix pack files.
10. On the **Available Maintenance Package to install** page, select the update and fix pack files and click **Next**.
11. Click **Install**.
12. On the last page, click **Finish**. The packages are installed.

13. To link the Integrated Solutions Console update with the profile where the Asset Discovery for Distributed server will be installed, issue the following command:
    - Linux UNIX `manageprofiles.sh –augment -profileName` *`profile_name`* `–templatePath /opt/IBM/WebSphere/AppServer/profileTemplates/iscae71/`
    - Windows `manageprofiles.bat –augment –profileName` *`profile_name`* *`-templatePath`* *`\was_install_dir`*`\IBM\WebSphere\AppServer\profileTemplates\iscae71\`

To verify whether the Integrated Solutions Console is updated and working, confirm that the **My Startup Pages** item and **Settings** node are visible in the left-hand navigation panel of the user interface. The **Settings** item should also be open in tabs. Additionally, on the navigation bar there should be "one-click expand/roll" button.

You can also check the output from:

- Linux UNIX *`websphere_application_directory`*`/bin/historyInfo.sh`
- Windows *`websphere_application_directory`*`/bin/historyInfo.bat`

to find out whether the feature 6.1.0.11-WS-WASFeature-FEISCAE7107.pak is installed.

You are now ready to extract the Asset Discovery for Distributed installation files.

Creating a dedicated profile in WebSphere Application Server V6.1:

Create a new dedicated profile for Asset Discovery for Distributedbto ensure that the product is separate from other applications installed on the WebSphere Application Server, and that it can be configured or uninstalled independently.

1. You can use and existing profile if no other application than Asset Discovery for Distributed uses it.
   To create a new profile, issue the following command:

   ```
   manageprofiles.bat -create -templatePath
   template_path    -profileName
   profile_name    -profilePath
   profile_path    -cellName
   cell_name      -nodeName
   node_name      -serverName server_name
   ```

   A message confirms that the profile was successfully created.
2. (Recommended) Back up your profile -this will enable you to return to the configuration from before performing the task. Issue the following command:

   ```
   manageprofiles.bat -backupProfile -profileName
   profile_name    -backupFile
   backup_file_path
   ```

   If you performed a backup of your profile, you can restore it by issuing the following command:

   ```
   manageprofiles.bat -restoreProfile - backupFile
   backup_file_path
   ```

Remember: Before you restore your profile, you need to delete it from WebSphere Application Server. You can do it with the `manageprofiles.bat -delete -profileName profile_name` command. You also need to delete the directory where the profile is located.

Extracting the installation files from the interactive installer:

Use the Asset Discovery for Distributed installation wizard to extract the files needed for upgrading the server and command-line interface.

Before you begin

Ensure that you have created and augmented the Asset Discovery for Distributed WebSphere Application Server profile.

To do this task:

1. Run **launchpad.exe** (Windows) or **launchpad.sh** (other platforms). The Welcome page opens.
2. In the left-hand navigation pane, click **Install or upgrade to Tivoli Asset Discovery for Distributed**.
3. Click **Launch the server installation wizard**.
4. Select the language of the installation and click **OK**. The installation wizard starts.
5. Click **Next**. After accepting the license agreement, click **Next** again.
6. Select **Production Environment** as the type of installation and proceed to the next page. This page opens only if no previous version of the product is discovered in the system.
7. On next panel select the **Unpack the files needed for manual deployment** option and specify the directory where you want to extract the files and click **Next**.
8. Specify the directory where you want to extract the files and click **Next**.
9. A progress indicator shows when the extract is complete. Click **Finish**.

The installer extracts the required installation files, including the keystore files `key.p12` and `trust.jks`, needed to enable secure communications between the server and its agents.

Note: If you enabled security before performing the upgrade, you should obtain the keystore files from the existing runtime installation.

The installation package contains the installation files, keystore files, JDBC driver files and the command-line interface. You can delete the .ear and .war installation files after you have deployed them. However, you must retain keystore files, JDBC driver files and the command-line interface files. It is recommended that you move them to the Asset Discovery for Distributed installation directory for easy reference.

Installing the server components:

After extracting the installation files and editing the SetupWAS.properties file, you are ready to install the Asset Discovery for Distributed server by running the scripts that you extracted.

Before you begin

Important: The scripts used in this method are only sample scripts. Before using them, check if they meet your requirements and modify them, if necessary.

Tip: If security is enabled on the WebSphere Application Server, you can specify your user name and password in the `soap.client.props` file in the properties directory of your WebSphere Application Server profile. To avoid any security risks, you can then additionally encrypt the file using the **PropFilePasswordEncoder** utility. See the WebSphere Application Server information center for more information.

To do this:

1. Copy the files `com.ibm.license.mgmt.msghandler.ear` and `tad4d_admin.war`, and the directory `WAS-scripts` from the directory where you extracted the installation files to the computer where WebSphere Application Server is installed. The directory `WAS-scripts` contains the following scripts:

   installAdmin.jacl
   Installs the administration component.

   installMessageHandler.jacl
   Installs the Message Handler component.

   setupDataSources.jacl
   Configures Data Sources and data base authentication.

   setupTimerManager.jacl
   Configures Timer Managers.

   setupTivoliCommonDir.jacl
   Configures Tivoli Common Directory.

   setupServerSecurePorts.jacl
   Configures the communication between the server and agents.

   setupWebContainer.jacl
   Sets up the Web container (for WebSphere Application server?).

2. Open a system command prompt and run the following command:

   - Windows **setupWAS.bat** *PATH_TO_WAS_PROFILE_DIRECTORY* [-log log_file_path]

     Note: On Windows, the path to the WAS profile directory should be provided within double quotation marks.

     An example of profile_path:

     ```
     ./setupWAS.bat "C:/Program Files/IBM/WebSphere/AppServer/profiles/
     AppSrv01"
     ```

   - Linux UNIX **setupWAS.sh** *PATH_TO_WAS_PROFILE_DIRECTORY* [-l log log_file_path]

   where *PATH_TO_WAS_PROFILE_DIRECTORY* is the path to the WebSphere Application Server profile directory.

   An example of profile_path:

   `./setupWAS.sh /opt/IBM/WebSphere/AppServer/profiles/AppSrv01/`If you do not specify the log file, the default `SetupWAS.log` file will be used. The scripts may take a few minutes to finish.

3. Restart WebSphere Application Server.

Enable the command-line interface.

Editing the SetupWAS.properties file:

Before deploying the Tivoli Asset Discovery for Distributed server, edit the `SetupWAS.properties` file to reflect your hardware and infrastructure. To ensure the success of your deployment, it is important to provide accurate data in this file.

Before you begin

You need to collect the configuration and security information about your WebSphere Application Server installation that is described in the following steps.

You will also need the database deployment details such as host name or IP address of the machine where DB2 is installed, database port number, user name and password.

Provide the following information in the `Setup.properties` file by performing the following steps:

1. Open the `SetupWAS.properties` file in a text editor.
2. Specify all of the following values:
   a. A path to directory that contains JDBC drivers (db2cc.jar, db2jcc_license_cu.jar).

      Example: **jdbcLocation=**`C:\Program Files\IBM\WebSphere\AppServer\JDBCdrivers\`

      The drivers are unpacked together with other files needed for deployment.
   b. Name of WebSphere Application Server cell and server node.

      Example: **cellName=***nc044112Node01Cell*

      Example: **nodeName=***nc044112Node01*

      Tip: You can obtain the cell name and the node name from the name of your WebSphere Application server profile. For example, if your profile is Windows `C:\Program Files\IBM\WebSphere\AppServer\profiles\AppSrv01\config\cells\nc044184Node01Cell\nodes\nc044184Node01\`, the *nc044184Node01Cell* value is the name of the cell, and the *nc044184Node01* is the name of the node.
   c. Name of the WebSphere Application Server server.

      Example: **serverName=***server1*

      server1 is the default server.
   d. WebSphere Application Server installation directory, for example:
      - Windows **wasHome=**`C:/Program Files/IBM/WebSphere/AppServer`
      - UNIX **wasHome=**`/opt/IBM/WebSphere/AppServer`
   e. Path to the directory that contains the admin package (`tad4d_admin.war`).
   f. Path to the directory that contains the `com.ibm.license.mgmt.msghandler.ear` package.
   g. Domain name or IP address of the host, where the database is installed.

      Example: **dbHostName=***localhost*
   h. Database port number.

      Example: **dbPortNumber=***50000*
   i. Name of database user.

Example: **dbUser=***tlmsrv*

j. Password for the database user. Specify a temporary password and delete it after deployment or provide the password during installation when a pop-up window appears.

   Example: **dbPassword=***xxxxxxx*

k. Full path to the keystore files (`key.p12`, `trust.jks`).

   In case of upgrading security-enabled environment keystore files should be obtained from Tivoli License Compliance Manager runtime server. For information on how to prepare the keystore files see the *Security* section of the information center.

l. Port for minimum security level transport:

   Default: **minSecurityPort=***9988*

m. Port for medium security level transport:

   Default: **minSecurityPort=***9999*

n. Port for maximum security level transport:

   Default: **minSecurityPort=***9977*

3. Save the file.

Resuming a stopped installation:

Script execution can sometimes fail, for example because of incorrectly supplied parameters, or because WebSphere Application Server was not started. In case of failure the script will report which step has failed and a how to resume execution at the given step.

Before you begin

Remove the `tad4d_admin.war` file from the isclite.ear directory in the WebSphere installation folder. This will allow you to rerun the script without any modifications.

Ensure that the `setupWAS.properties` file is correctly filled up, and that WebSphere Application Server is running.

By default, the setup script logs into the file `SetupWAS.log` in the current directory. The log file can be specified by using switch -log command on Windows or switch -l one on Unix.

The general command syntax for resuming the installation is as follows:

- for `setupWAS.bat` (Windows):

  ```
  setupWAS.bat profile_path [-step step_id] [-log log_file_path]
  ```

  where `-step` resumes execution at a given step, and `-l` logs you into a given file (the default log file SetupWAS.log in current directory).

  Note: On Windows, the path to the WAS profile directory should be provided within double quotation marks.

  An example of profile_path:

  ```
  ./setupWAS.bat "C:/Program Files/IBM/WebSphere/AppServer/profiles/
  AppSrv01" -step setupDataSources
  ```

- for `setupWAS.sh` (other platforms):

  ```
  setupWAS.sh profile_path [-s step_id] [-l log_file_path]
  ```

where -s resumes execution at a given step, and -l logs you into a given file (the default log file SetupWAS.log in current directory).

An example of profile_path:

```
./setupWAS.sh /opt/IBM/WebSphere/AppServer/profiles/AppSrv01/ -step
setupDataSources
```

1. Check the log file to find the root cause of the failure.
2. Fix the problem.
3. Resume the installation at the step that failed by running the setup script:
   - UNIX `setupWAS.sh` *profile_path* -s *step_id* -l *-log log_file_path*
   - Windows `setupWAS.bat` *profile_path* -step *step_id -log log_file_path*

   Note: If after performing the described procedure, the installation fails, perform the undeployment procedure, and start a new installation.

The installation resumes.

Manually installing the server components:

If you are installing Asset Discovery for Distributed server on a stand-alone version of WebSphere Application Server, you can choose to install and configure the server components manually.

Before you begin

This procedure has the following prerequisites:

- Supported versions of IBM DB2 and WebSphere Application Server, plus required fix packs, are already installed.
- You are an experienced administrator in both of those environments.

This installation scenario is intended for large enterprise customers. It includes the following tasks:

Installing the administration and Message Handler components:

Manual installation of the Asset Discovery for Distributed server server components starts with deployment of two archive files. A Web archive (WAR) file contains the administration component of the application, including the user interface, and an enterprise archive (EAR) file contains the message handler for communication between the server and agents. If have decided not to use the scripts provided for server installation, you must install these two components from the wsadmin scripting console.

This task is part of the installation scenario for manually installing the server components. It is intended for large enterprise customers with advanced administration skills.

Note: If WebSphere Application Server is running during the installation process, numerous exceptions and error messages will be logged in WebSphere Application Server log files. This is expected and you should treat it as feedback about successful installation.

To install the two components, perform the following steps:

1. Issue the following wsadmin command to install the administration component: `$AdminApp update isclite modulefile [list -operation add -contents admin_path -contenturi admin_war -custom paavalidation=true -usedefaultbindings -contextroot /ibm/lmt -MapWebModToVH {{.* .* admin_host}}]` where the `admin_path` is the path to the administration application Web component and `admin_war` is the name of the administration Web component file, by default `tad4d_admin.war`.
2. Save the configuration by issuing the `$AdminConfig save` command.
3. Install the Message Handler by issuing the following command: `$AdminApp install msghandler_ear [list -cell cell_name -node node_name -server server_name]`, where `msghanler_ear` is the path to the Message Handler ear file, `com.ibm.license.mgmt.msghandler.ear` by default. The `cell_name`, `node_name`, `server_name` are names of the cell, node, and server where you want the Message Handler to be installed.
4. Run the `$AdminConfig save` command to save the configuration. Error messages that may appear in the log files as a result of this operation are expected and should be treated as positive feedback.

Now, you need to create the connection between the server and the database.

Configuring the connection between the server and the database:

Asset Discovery for Distributed server uses the DB2 database as data storage. Define the connection between the server and the DB2 database.

1. Create Java™ Database Connectivity (JDBC) provider.
2. Create the JAASAuthData object.
3. Create the data sources.

Creating Java Database Connectivity (JDBC) provider:

Communication between the Tivoli Asset Discovery for Distributed server and database requires a JDBC provider and a data source.

Before you begin

This installation scenario has the following prerequisites:

- You have installed the administration and message handler components of the Asset Discovery for Distributed server server.
- You have installed a supported version of DB2 and any corequisite fix packs.

This task is part of the installation scenario for manually installing the server components. It is intended for large enterprise customers with advanced administration skills.

The provider needs to have the following properties:

Table 26. JDBC provider properties

Parameter	Value
name	*Arbitrary name* for example *MyJDBCProvider*
implementationClassName	`com.ibm.db2.jcc.DB2ConnectionPoolDataSource`

Table 26. JDBC provider properties (continued)

Parameter	Value
classpath	*DIRECTORY_WITH_EXTRACTED_SCRIPTS*/jdbc/db2jcc.jar; *DIRECTORY_WITH_EXTRACTED_SCRIPTS*/jdbc/db2jcc_license_cu.jar
xa	*false*
nativePath	null

Run the scripts to create the JDBC provider. The following script is an exemplary script that creates a provider with the parameters described in the table above:

```
set server [$AdminConfig getid /Cell:cell_name/Node:node_name/Server:server_name/]
$AdminConfig create JDBCProvider $server
{
{name provider_name}
{implementationClassName "com.ibm.db2.jcc.DB2ConnectionPoolDataSource"
}
{classpath "DIRECTORY_WITH_EXTRACTED_SCRIPTS/jdbc/db2jcc.jar;
DIRECTORY_WITH_EXTRACTED_SCRIPTS/jdbc/db2jcc_license_cu.jar"}
{xa false}
}
```

The `cell_name`, `node_name`, and `server_name` are the name of the cell, node, and server where you want the Message Handler installed. The `provider_name` is an arbitrarily chosen name of the JDBC provider that you are creating.

Now, you can move on to create the JAASAuthData object.

Creating the JAASAuthData object:

The JAASAuthData object contains the credentials for the tlmsrv user ID that the administration server uses to connect to the Asset Discovery for Distributed server. You must create this object before creating any data sources.

This task is part of the installation scenario for manually installing the server components. It is intended for large enterprise customers with advanced administration skills.

The JAASAuthData object needs to have the following properties:

Table 27. JAASAuthData properties

Parameter	Value
alias	*Arbitrary name*
userId	*tlmsrv*
password	*tlmsrv_password*

Run a script to create the JAASAuthData object. The following script creates an JAASAuthData object with properties listed in the table above:

```
set security [$AdminConfig getid /Cell:cell_name/Security:/]
$AdminConfig create JAASAuthData $security { {alias auth_alias}
{userId tlmsrv} {password tlmsrv_password} }
```

The `cell_name` is the name of the cell where you want to deploy the application, the `auth_alias` is an arbitrarily chosen name of the alias (for example `my_alias`), and the `tlmsrv_password` is the password for the tlmsrv database user.

Now, you can create the data sources.

Creating the data sources:

The data sources are necessary to finish configuring the connection between the server and the database. Create the data sources with specific properties.

This task is part of the installation scenario for manually installing the server components. it is intended for large enterprise customers with advanced administration skills.

1. To create the TLMA data source, adapt the sample script shown below, substituting your own values as indicated in the following table:

Table 28. TLMA data source parameters

Parameter	**Value**		
name	*ds_name*		
datasourceHelperClassname	`com.ibm.websphere.rsadapter.DB2UniversalDataStoreHelper`		
jndiName	`jdbc/TLMA`		
propertySet	**name**	**value**	**type**
	`databaseName`	`TLMA`	`java.lang.String`
	`serverNumber`	*server_addr*	`java.lang.String`
	`portNumber`	*port_number*	`java.lang.Integer`
	`driverType`	*4*	`java.lang.Integer`
connectionPool	**name**	**value**	
	`maxConnections`	*50*	
mappings	**name**	**value**	
	`authDataAlias`	*auth_alias*	

You can use the following script to do this:

```
set provider [$AdminConfig getid /Cell:cell_name/Node:node_name/Server:server_name/JDBCProvide
set ds [$AdminConfig create DataSource $provider [list [list name ds_name] [list jndiName jdbc
$AdminConfig create J2EEResourcePropertySet $ds [list [list resourceProperties [list [list [li
$AdminConfig create MappingModule $ds {{authDataAlias auth_alias}}

set pool [$AdminConfig showAttribute $ds connectionPool]

$AdminConfig modify $pool { {maxConnections 50} }
```

The following parameters are used in this command:

cell_name, node_name, server_name
The names of the cell, node and server where you want to deploy the application.

provider_name
The name of the previously created JDBC provider.

server_addr
The address of the server where the database is installed.

port_number
The port to be used to communicate with the database.

auth_alias
Previously created authentication alias.

2. To create the TLMA_MsgHandler data source, adapt the sample script shown below, substituting your own values as indicated in the following table:

Table 29. TLMA_MsgHandler data source properties

Parameter	**Value**		
name	*Msghandler_ds_name*		
datasourceHelperClassname	`com.ibm.websphere.rsadapter.DB2UniversalDataStoreHelper`		
jndiName	`jdbc/TLMA_MsgHandler`		
propertySet	**name**	**value**	**type**
	databaseName	*TLMA*	*java.lang.String*
	serverName	*server_addr*	*java.lang.String*
	portNumber	*port_number*	*java.lang.Integer*
	driverType	*4*	*java.lang.Integer*
conectionPool	**name**	**value**	
	`maxConnections`	`101`	
mappings	**name**	**value**	
	`authDataAlias`	*auth_alias*	

Below, there are exemplary scripts that create the TLMA_MsgHandler data source with the properties listed in Table 2. Because of the similarity to the TLMA data source, the TLMA data source can be used as a template:

```
set provider [$AdminConfig getid /Cell:cell_name/Node:node_name/Server:server_name/JDBCProvider:p
set msghandler_ds [$AdminConfig createUsingTemplate DataSource $provider {{name msghandler_ds_nam
set pool [$AdminConfig showAttribute $msghandler_ds connectionPool]
$AdminConfig modify $pool { {maxConnections 101} }
```

The parameters that are used in this command are:

cell_name, node_name, server_name
The names of cell, node and server where you want to deploy the application.

provider_name
The name of the previously created JDBC provider.

ds_name
The name of the previously created TLMA data source.

msghandler_ds_name
The name of the TLMA_MsgHandler data source.

3. To create the TLMHW data source, adapt the sample script shown below, substituting your own values as indicated in the following table.

Table 30. TLMHW data source properties.

Parameter	**Value**
name	*tlmhw_ds_name*
datasourceHelperClassname	`com.ibm.websphere.rsadapter.DB2UniversalDataStoreHelper`
jndiName	`jdbc/TLMA_MsgHandler`

Table 30. TLMHW data source properties. (continued)

Parameter	Value		
propertySet	**name**	**value**	**type**
	databaseName	TLMA	java.lang.String
	serverName	*server_addr*	java.lang.String
	portNumber	*port_number*	java.lang.Integer
	driverType	4	java.lang.Integer
mappings	**name**	**value**	
	authDataAlias	*auth_alias*	

You may use the scripts below to create the TLMHW data source:

```
set provider [$AdminConfig getid /Cell:cell_name/Node:node_name/
Server:server_name/JDBCProvider:provider_name/]
set ds [$AdminConfig getid /Cell:cell_name/Node:node_name/
Server:server_name/JDBCProvider:provider_name/DataSource:ds_name]
set tlmhw_ds [$AdminConfig createUsingTemplate DataSource
$provider {{name tlmhw_ds_name} {jndiName jdbc/TLMHW}} $ds]
```

The parameters used in this command are:

cell_name, node_name, server_name
The names of the cell, node and server where you want to deploy the application.

provider_name
The name of the previously created JDBC provider.

ds_name
The name of the previously created TLMA data source.

tlmhw_ds_name
The name of the previously created TLMA_MsgHandler data source.

Configuring the communication between the agent and the Message Handler:

Configure ports and prepare server certificates to enable the set up the agent-Message Handler communication and enable the Tivoli Asset Discovery for Distributed agent to transport collected data to the server. You must specify one of the three security levels for agent-to-server communications. The three levels are minimum, medium or maximum. Each level requires a different HTTP or HTTPS port.

This task is a part of the installation scenario for manually installing the server components. It is intended for large enterprise customers with advanced administration skills.

1. Create the thread pool for communication threads. Ensure that the thread pool has the following parameters:

Table 31. The thread pool parameters

Parameter	Value
name	*pool_name*
maximumSize	*50*

You can use the following script to create such thread pool:

```
set manager [$AdminConfig getid /Cell:cell_name/Node:node_name/Server:server_name/ThreadPoolManag
$AdminConfig create ThreadPool $manager [list [list name pool_name] [list maximumSize 50]]
```

Where the **cell_name**, **node_name**, and **server_name** are the names of the cell, node and server where you want to deploy the application; the **pool_name** is the name of the pool that you want to create, for example **my_pool**.

2. Create transport endpoints and associate them with specified ports and specified SSL configuration objects.
   a. Create keystore and truststore.
   b. Create the SSL configuration objects.

Creating keystore and truststore:

Communication over Secure Sockets Layer (SSL) requires a keystore to store the server certificate delivered with the application, and a truststore for the client certificate. If you have chosen to install and configure the server components of Asset Discovery for Distributed server manually, you need to create keystore and truststore objects that associate the SSL configuration objects with proper transport endpoints.

This task is part of the installation scenario for manually installing the server components. It is intended for large enterprise customers with advanced administration skills.

1. To create the keystore, run the following command:: `$AdminTask createKeyStore [list -keyStoreName key_store_name -keyStoreType type -keyStoreLocation key_store_path -keyStorePassword password -keyStorePasswordVerify password -scopeName (cell):cell_name:(node):node_name]`. The variables have the following values:

   key_store_name
   An arbitrarily chosen name of the keystore, for example **my_key_store**.

   type
   The type of the keystore file.

   key_store_path
   The path to the file containing keystore.

   password
   The password to the keystore.

   cell_name, node_name, server_name
   The names of the cell, node and server accordingly where you want to deploy the product.

   Note: The server certificate is delivered by default with the product in the .p12 format. The type to be used with the keystore is PKCS12.

2. Create the truststore by issuing the `$AdminTask createKeyStore [list -keyStoreName trust_store_name -keyStoreType type -keyStoreLocation trust_store_path -keyStorePassword password -keyStorePasswordVerify password -scopeName (cell):cell_name:(node):node_name]` command. The parameters used in the command are:

   trust_store_name
   An arbitrarily chosen name of the truststore, for example **my_trust_store**.

   type
   The type of the keystore file.

trust_store_path
The path to the file containing truststore

password
The password to the truststore

cell_name, node_name, server_name
The names of the cell, node and server accordingly where you want to deploy the product.

Note: Because the client certificate stored in the truststore is in the JKS format, the type to be used with the truststore is JKS.

Now, you can create the SSL configuration objects.

Creating the SSL configuration objects:

The Secure Sockets Layer (SSL) creates a secure communication between the agent and the server.

This task is part of the installation scenario for manually installing the server components. It is intended for large enterprise customers with advanced administration skills.

1. Issue the following command to create the SSL object for server authentication: `$AdminTask createSSLConfig [list -alias alias -scopeName (cell):cell_name:(node):node_name -clientKeyAlias client_alias -serverKeyAlias server_alias -trustStoreName trust_store_name -trustStoreScopeName (cell):cell_name:(node):node_name -keyStoreName key_store_name -keyStoreScopeName (cell):cell_name:(node):node_name]`. The command uses the following parameters:

   alias
   An arbitrary alias of the configuration object.

   cell_name, node_name
   The names of the cell and node as a scope for the corresponding objects.

   client_alias
   An arbitrary client alias.

   server_alias
   An arbitrary server alias.

   trust_store_name
   The name of the defined truststore.

   key_store_name
   The name of the defined keystore.
2. Issue the `$AdminTask createSSLConfig [list -alias alias -scopeName (cell):cell_name:(node):node_name -clientKeyAlias client_alias -serverKeyAlias server_alias -trustStoreName trust_store_name -trustStoreScopeName (cell):cell_name:(node):node_name -keyStoreName key_store_name -keyStoreScopeName (cell):cell_name:(node):node_name -clientAuthentication true -securityLevel HIGH -jsseProvider IBMJSSE2 -sslProtocol SSL_TLS]` command to create the SSL configuration object for server and client authentication. The command uses the following parameters:

   alias
   An arbitrarily chosen alias of the configuration object.

cell_name, node_name
The names of the cell and node as a scope for the corresponding objects.

client_alias
An arbitrarily chosen client alias.

server_alias
An arbitrarily chosen server alias.

trust_store_name
The name of the defined truststore.

key_store_name
The name of the defined keystore.

3. Create the endpoints together with the ports for communication.
   a. Create the endpoint for non-secure (HTTP) communication. The HTTP endpoint should have the following properties:

Table 32. HTTP endpoint properties

Parameter	Value	
endPointName	*min_security_end_point_name*	
	Parameter	**Value**
endPoint	*host*	*
	port	*min_security_port*

You can use the following script to create this endpoint:

```
set channel [$AdminConfig getid /Cell:cell_name/Node:node_name/Server:server_name/TransportCha

set endPoint [$AdminTask createTCPEndPoint $channel [list -name min_security_end_point_name -
```

The **cell_name**, **node_name**, and **server_name** are the names of the cell, node, and server as a scope for the corresponding objects. The **min_security_end_point_name** is the arbitrary chosen name for this endpoint, and the **min_security_port** is the port that is to be used for HTTP communication.

   b. Associate the thread pool with the TCP channel to create a chain for communication. Issue the following commands to do this: `set template [lindex [$AdminConfig listTemplates Chain WebContainer] 0]`
```
set chain [$AdminTask createChain $channel [list -template $template
-name chain_name -endPoint $endPoint]]
set pool [$AdminConfig getid /Server:serverManual/ThreadPoolManager:/
ThreadPool:pool_name/]
set channels [split [lindex [$AdminConfig showAttribute $chain
transportChannels] 0] " "]
set tcp [lindex $channels [lsearch -regexp $channels TCP*]]
$AdminConfig modify $tcp [list [list threadPool $pool]]
```
   c. Issue the `set virtualHost [$AdminConfig getid /Cell:cell_name/ VirtualHost:default_host/] $AdminConfig create HostAlias $virtualHost [list [list hostname *] [list port min_security_port]]` command to create virtual host associated with the port used for above TCP transport channel. The following parameters are used in this command:

cell_name, node_name, server_name
The names of the cell, node and server as a scope for the corresponding objects.

chain_name
An arbitrarily chosen name of the communication chain.

pool_name
The name of the thread pool that was previously created.

min_security_port
The port that is to be used for HTTP communication.

Creating timer managers:

The Tivoli Asset Discovery for Distributed server processes large amounts of data in asynchronous mode by using WebSphere Application Server's timer managers, also known as *asynchronous beans*. You need to create two timer managers in order for the server to process the data.

This task is part of the installation scenario for manually installing the server components. It is intended for large enterprise customers with advanced administration skills.

Two timer managers are required to enable the server to process the data. The timer managers need to have the following properties:

Table 33. Timer manager1 properties

Parameter	Value
name	*manager_name*
jndiName	*tm/TAD4D_Timer1*
numAlarmThreads	*1*

Table 34. Timer manager 2 properties

Parameter	Value
name	*manager_name*
jndiName	*tm/TAD4D_Timer2*
numAlarmThreads	*1*

1. Issue the following command to create first timer manager:

```
set timerMgrProvider [$AdminConfig getid /Cell:cell_name/Node:node_name/Server:server_name/Tim
$AdminConfig create TimerManagerInfo $timerMgrProvider {{name timer_name1} {jndiName tm/LMT_Ti
```

   The following parameters were used in this command:

   cell_name, node_name, server_name
   The names of the cell, node and server as a scope for the corresponding objects.

   timer_name1
   Arbitrarily chosen name of this time manager.

2. Create another timer manager by issuing the following command:

```
set timerMgrProvider [$AdminConfig getid /Cell:cell_name/Node:node_name/Server:server_name/Tim
$AdminConfig create TimerManagerInfo $timerMgrProvider {{name timer_name2} {jndiName tm/LMT_Ti
```

   The following parameters are used in the command:

cell_name, node_name, server_name
The names of the cell, node and server as a scope for the corresponding objects.

timer_name2
Arbitrarily chosen name of this time manager.

Defining Java properties:

If you choose to install the Asset Discovery for Distributed server components manually instead of from scripts, set Java properties to prevent the application server from using too much memory and to improve the data transfer. There are two objects whose properties you need to set: the Java Virtual Machine (JVM) configuration object that is associated with the server where you want to install the application, and the Web container.

This task is part of the installation scenario for manually installing the server components. It is intended for large enterprise customers with advanced administration skills.

To set the properties of these objects:

1. Run the scripts to set the Java Virtual Machine configuration object properties. The parameters of this object should have the following values:

Table 35. Java Virtual Machine configuration object properties

Parameter	Value
Windows **W32ProgFilesDir**	*program_files_dir*
TCDAlwaysGetCommonDir	*false*

The following scripts are exemplary scripts setting these values:

```
set server [$AdminConfig getid /Cell:cellManual/Node:nodeManual/Server:serverManual/]
set jvm [lindex [$AdminConfig list JavaVirtualMachine $server] 0]
```

Windows

```
$AdminConfig modify $jvm [list [list systemProperties [list [list [list name W32ProgFilesDir] [li
```

UNIX

```
$AdminConfig modify $jvm [list [list systemProperties [list [list [list name TCDAlwaysGetCommonDi
```

2. Set the Web container **com.ibm.ws.webcontainer.channelwritetype** parameter to *sync*. You can use the following script to do it:

```
set container [$AdminConfig list WebContainer $server]
$AdminConfig modify $container [list [list properties [list [list [list name com.ibm.ws.webcontai
```

Now that you have performed all the steps necessary to install the server, check if the installation completed successfully.

Verifying the configuration process:

After you have performed all the steps of manual installation on the base version of the WebSphere Application Server, you need to verify if the configuration was successful.

Before you begin

Ensure that you have restarted the server after completing all of the configuration tasks.

This task is part of the installation scenario for manually installing the server components. It is intended for large enterprise customers with advanced administration skills.

To verify the configuration:

1. Access the Web user interface at the following address: `http(s)://server_ip:port_number/ibm/console`. If you can access the Web user interface without any problems, it means that the installation was successful.
2. Check the log files for error messages. You can find the log files under the following locations: *`Tivoli_Common_Directory`*`/COD/logs/` or *`profile_path`*`/logs/`*`server_name`*`/`. The *profile_path* is the path to the Websphere Application Server profile where the application is deployed, and the *server_name* is the name of the server where the application is deployed.

Enabling the Tivoli Asset Discovery for Distributed command line interface:

Having installed the server components you must now proceed to enabling Tivoli Asset Discovery for Distributed command line interface.

Before you begin

You need to extract the files for the manual installation of Asset Discovery for Distributed as described in "Extracting the installation files from the interactive installer" on page 66. Ensure that you have moved the Tivoli Asset Discovery for Distributed command-line interface files to the product installation directory to be able to locate them easily in the future.

To do this:

1. Locate the **`cli`** directory that you created when moving the extracted deployment files from the interactive installer.
2. In the `conf` subdirectory of the `directory` directory, open the cli.properties file for editing. Supply the following information:

   Supply the following information:

   secureAdminPort=
   The number of the secure administration port

   Example: Windows UNIX secureAdminPort=9044

   This is the same port that you can use to access the secure Web user interface.

   trustStorePath=
   The path to the keystore file (`trust.p12`)

   Example:

   - Windows trustStorePath=`C:/Program Files/IBM/WebSphere/AppServer/profiles/AppSrv01/config/cells/nc044112Node01Cell/nodes/nc044112Node01/trust.p12`

- UNIX trustStorePath=/usr/IBM/WebSphere/AppServer/profiles/LmtSrv01/config/cells/NC047014Node02Cell/nodes/NC047014Node02/trust.p12

3. If WebSphere Application Server was installed in a location other than the default, you also need to edit the `lmtcli.sh` or `lmtcli.bat` file.

   Supply the following information:

   WAS_HOME=
   The path to the used WAS_HOME (if it is different than the standard one).

   Example:

   - Windows WAS_HOME=C:/Program Files/IBM/WebSphere/AppServer
   - UNIX WAS_HOME=/opt/IBM/WebSphere/AppServer

4. Ensure that WebSphere Application Server security is enabled. For more information, see the "Security" section of the information center.
5. To start the command line interface run the command:

   - Windows **lmtcli.bat**
   - UNIX **lmtcli.sh**

   Note: Before running the command on Unix platform, execution right must be granted by running the **chmod u+x lmtcli.sh** command.

6. Login to the Tivoli Asset Discovery for Distributed command line interface as System Administrator and perform some commands to verify that the settings are correct. For more information about accessing the command-line interface and about the login command, refer to the "Reference" section of the information center.

Now you can verify if the enabling of the command line interface was successful by running a few basic commands.

Forwarding data from agents to Tivoli Asset Discovery for Distributed server

Because there are no more runtime servers in Asset Discovery for Distributed infrastructure, you need to enable *data forwarding* for existing License Compliance Manager agents in your infrastructure.

Before you begin

Enable data forwarding if you have previously decided to use the existing, version 2.3 agents.

Choose the solution to forward data that best suits your needs. You have three possibilities:

- Set up proxy servers that will perform the role of data forwarders. The process differs depending on what type of application server you have installed. The two options are:
  - "Configuring IBM HTTP server to forward data traffic from agents to a stand-alone WebSphere Application Server" on page 83
  - "Configuring IBM HTTP server to forward data traffic from agents to the embedded WebSphere Application Server" on page 86
- Modify host names in the Domain Name Services server in your infrastructure

- Re-configure agents to send data directly to the Asset Discovery for Distributed server

The infrastructure architecture with proxy servers performing the data forwarding function

You can set up proxy servers as one of the solutions to forward data from V.2.3 agents to theTivoli Asset Discovery for Distributed server.

Proxy servers that perform the data forwarding function are HTTP servers with binary plug-ins installed in them. Proxy servers need to be defined in the Asset Discovery for Distributed WebSphere Application Server.

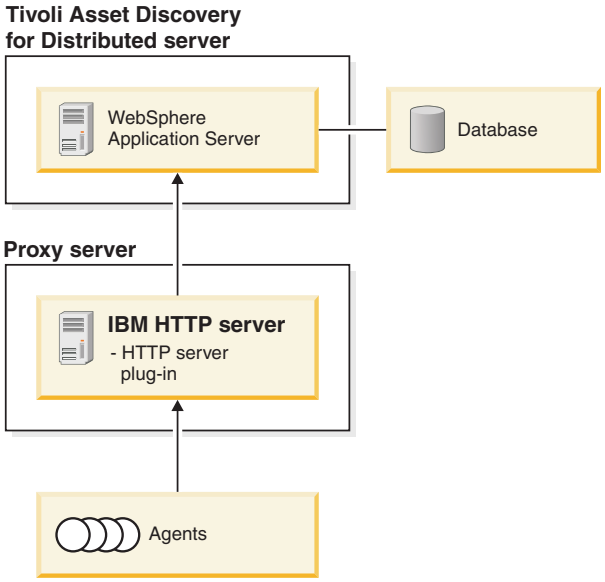
The following are the elements of the proxy servers architecture (starting from the top):

Proxy servers definitions in WebSphere Application Server
: You can create the definitions using the Integrated Solutions Console user interface (installing on top of base WebSphere Application Server) or a script can create the definitions (installing with the embedded version of WebSphere Application server).

HTTP server with a binary plug-in installed in it
: You can generate the plugin using the Integrated Solutions Console user interface or a script will generate it. Proxy servers can be enabled on computers that performed the role of runtime servers or on new computers.

  Note: It is recommended to use the IBM HTTP server.

Tivoli License Compliance Manager Version 2.3 agents
: These agents have not been configured to send data directly to the new Asset Discovery for Distributed server.



Configuring IBM HTTP server to forward data traffic from agents to a stand-alone WebSphere Application Server

If you installed Asset Discovery for Distributed on base IBM WebSphere Application Server rather than the embedded version, and if you do not plan to

upgrade existing License Compliance Manager agents right away, install a plug-in that enables a proxy server on each computer that is to perform data forwarding. Proxy servers send data from your old agents to your new administration server.

A proxy server works with the HTTP server software that may still be installed anywhere you uninstalled the runtime server component of License Compliance Manager.

Before you begin

- You must have the following operating system privileges:
  - Windows Administrator
  - UNIX root
- You require the IBM HTTP Server administrator user name and password.
- Keystores should be configured on the Tivoli Asset Discovery for Distributed server.
- Linux UNIX You require the User ID and group for the catalog where the plugin and configuration file are located.
- The administration server on the remote system (where the HTTP server is installed) must be running. Start the server:
  - UNIX By issuing thew command: `/opt/IBM/HTTPServer/bin/adminctl start`
  - Windows By navigating the Start menu: **Start → IBM HTTP Server V6.1/ → Start Admin Server**

To do this:

1. On the computer where you have just installed Asset Discovery for Distributed log on to the Integrated Solutions Console.
2. In the navigation pane, expand the **ServersWeb servers**. When the Web servers pane opens, click the **New** push button.
3. A wizard guides you through the web server configuration process. On the first page, supply the following information:

   Server name
   This must be the same name that you provided during the installation of the HTTP server. Provide the name to propagate the plugin. By default it is `webserver1`, especially if the runtime server was formerly installed on the same machine as the administration server.

   Type Leave the default value, `IBM HTTP Server`.

   Host name
   Provide the IP address or unique host name of the computer that you have chosen to forward the data traffic from agents to the Asset Discovery for Distributed server (and which had earlier performed the role of runtime server).

   Platform
   In the drop down menu, choose the platform that the *proxy server* will be installed on. In this example, the Windows platform is used.

   Click **Next**.
4. Select a **IHS** Web server template and click **Next**.

5. On the new pane **Step 3: Enter the properties for the new Web server** supply the following information:

   Windows **Web Server properties**

   Service name
   Provide the name of the process that runs IBM HTTP server in the Windows operating system

   Application mapping to the Web server
   Leave the default choice: **All**.

   Windows **Administration Server properties**

   Port Enter the port number that the Asset Discovery for Distributed server uses for communication with agents.

   Username
   Supply the IBM HTTP server administrator's username that was determined during the installation of the plugin. In case user was not provided earlier, it can be created on HTTP server machine in the following way:

   `htpasswd -cm` *`install_dir`*`\conf\admin.passwd` *`login name`*

   For the other settings, you can accept the defaults.

   Password
   Supply the IBM HTTP server administrator's password that was determined during the installation of the plugin.

   Confirm password
   Retype the IBM HTTP server administrator's password.

   AIX UNIX **Web Server properties**

   Port Provide port number that will be used for communication with Tivoli License Compliance Manager administration server Version 2.3 agents

   Web server installation location
   Provide full file path to the Web server directory

   Plug-in installation location
   Provide full file path to the Plug-in installation directory

   Application mapping to the Web server
   Leave the default choice: **All**.

   AIX UNIX **Administration Server properties**

   Port Enter the port number that the Asset Discovery for Distributed server uses for communication with agents.

   Username
   Supply the IBM HTTP server administrator's username that was determined during the installation of the plugin. In case user was not provided earlier, it can be created on HTTP server machine in the following way:

   `./htpasswd -cm` *`install_dir`*`/conf/admin.passwd` *`login name`*

   For the other settings, you can accept the defaults.

   Password
   Supply the IBM HTTP server administrator's password that was determined during the installation of the plugin.

Confirm password
Retype the IBM HTTP server administrator's password.

Click **Next**

6. On the last page of the wizard, click **Finish** button to complete the creation of web server definition. When a message confirms successful installation of the new server definition, click the **Save** link in the message.
7. In the Web servers table, select the Web server that you have created and then click **Generate Plug-in**. The plug-in has now been generated on the computer that will perform the role of proxy server.
8. Click **Propagate Plug-in**. Completion messages confirm the configuration has been sent to the new proxy server.
9. Restart the IBM HTTP server by issuing the command:
   - AIX

     `/usr/IBMIHS/bin/` **apachectl stop**

     `/usr/IBMIHS/bin/` **apachectl start**
   - UNIX

     `/opt/IBMIHS/bin/`**apachectl stop**

     `/opt/IBMIHS/bin/`**apachectl start**
   - Windows

     From the **Start menu**, select **IBM HTTP server** and **Stop HTTP Server**, then **Start HTTP Server**.

     You may also restart the server by pressing `Control+C` in the IBM HTTP Server window (to stop the server) and later by changing to the following directory and running the executable file:**<IHS_INSTALL_DIRECTORY>**`/bin/` **apache.exe**.

   After you restart the HTTP server, your existing License Compliance Manager agents can now communicate with the Asset Discovery for Distributed server.

As time permits, upgrade and re-configure your old License Compliance Manager agents to Asset Discovery for Distributed. When you have no more old agents to support, you can remove the proxy servers.

Configuring IBM HTTP server to forward data traffic from agents to the embedded WebSphere Application Server

If you installed Asset Discovery for Distributed on the embedded version of IBM WebSphere Application Server, and if you do not plan to upgrade existing License Compliance Manager agents right away, run a script to install a plug-in that enables a proxy server on each computer that is to perform data forwarding. Proxy servers send data from your old agents to your new administration server.

A proxy server works with the HTTP server software that is still installed anywhere you uninstalled the runtime server component of License Compliance Manager.

Before you begin

- You must have the following operating system privileges:
  - Windows Administrator
  - UNIX root
- You require the IBM HTTP Server administrator user name and password.

- Linux UNIX You require the User ID and group for the catalog where the plugin and configuration file are located.
- The administration server on the remote system must be running.

Run this script once for every runtime server that existed in your License Compliance Manager V2.3 environment.

To do this:

1. On the computer where you have just installed Asset Discovery for Distributed server copy the following script below to a text editor and modify the values (in bold), following the instructions contained within it:

```
##################################################
######EDIT THIS SCRIPT BEFORE YOU USE IT ! ! !########
##################################################
#Address of host on which you want plugin to be propagated
#for example localhost
#for example 9.156.44.183
set hostName 9.156.44.183

#Platform of server on which plugin will be propagated
#use lower case
#for example linux
set platform linux

#Webserver name, has to be the same as webserver name created during plugin installation
#for example webserver1
set webserverName webserver1

#Path to Http server installation on machine where you want plugin to be propagated
#for example /opt/IBM/HTTPServer
#for example "C:\\Program Files\\ibm\\HTTPServer"
set webInstallRoot  /opt/IBM/HTTPServer

#Plugin installation path of machine where you want plugin to be propagated
# /opt/IBM/HTTPServer/Plugins
#for example "C:\\Program Files\\ibm\\HTTPServer\\Plugins"
set pluginInstallRoot /opt/IBM/HTTPServer/Plugins

#Administration server port
#for example 8008
set adminPort 8008

#Administration server (Asset Discovery/License Metric Tool server) User ID
set adminUserID Admin

#Password
set adminPasswd myPassword

#Path to the embedded WebSphere Application Server software
#for example "C:\\Program Files\\ibm\\LMT\\eWas\\profiles\\AppSrv01\\config"
#for example /opt/IBM/LMT/eWas/profiles/AppSrv01/config
set eWasConfigPath "C:\\Program Files\\ibm\\LMT\\eWas\\profiles\\AppSrv01\\config"
################################################################################
#DO NOT EDIT WHAT IS BELOW
################################################################################


#-------------------------------------------------------------
# Check if the Web server opertating system is valid
#-------------------------------------------------------------
if { (!(($platform == "windows") || ($platform == "solaris") || ($platform == "aix") ||
 ($platform == "hpux") || ($platform == "linux") || ($platform == "os400")|| ($platform == "os390"))) } {

    puts ""
    puts "Invalid platform specified."
    return false
}


puts ""
puts "Creating Web server..."
if {[catch {$AdminTask createWebServerByHostName "-hostName $hostName -platform $platform -webserverName
$webserverName  -templateName IHS -webPort 80 -webInstallRoot $webInstallRoot -
pluginInstallRoot $pluginInstallRoot -configurationFile  -serviceName  -errorLogfile  -
accessLogfile  -webAppMapping ALL -adminPort $adminPort -adminUserID $adminUserID
-adminPasswd $adminPasswd"} result]} {
 puts "-----------------------------------------------------"
 puts "Web server definition for $webserverName is not created, read exception below."
 puts "-----------------------------------------------------"
 puts "exception = $result"
} else {
 puts "saving..."
 $AdminConfig save
}
```

```
set plg [$AdminControl completeObjectName WebSphere:*,type=PluginCfgGenerator]
set node $hostName-node

puts ""
puts "Generating plugin..."
if {[catch {$AdminControl invoke $plg generate [list $eWasConfigPath cell1 $node $webserverName
  false ] {java.lang.String java.lang.String java.lang.String java.lang.String java.lang.Boolean} } result]} {
 puts "------------------------------------------------------------"
 puts "Plugin was not generated, read exception below."
 puts "------------------------------------------------------------"
 puts "exception = $result"
 return -code error
} else {
 puts "------------------------------------------------------------"
 puts "Plugin generated successfully."
 puts "Plugin plugin-cfg.xml can be found in following folder:"
 set path "$eWasConfigPath\\cells\\cell1\\nodes\\$node\\servers\\$webserverName"
 puts "$path"
 puts "------------------------------------------------------------"
}


puts ""
puts "Propagating plugin..."
if {[catch {$AdminControl invoke $plg propagate [list $eWasConfigPath cell1 $node $webserverName]
 {java.lang.String java.lang.String java.lang.String java.lang.String} } result]} {
 puts "------------------------------------------------------------"
 puts "Plugin was not propagated, read exception below."
 puts "------------------------------------------------------------"
 puts "exception = $result"
 puts "------------------------------------------------------------"
 puts "Be sure that Http admin server is turned on."
 puts "You can copy plugin file manually."
 puts "plugin-cfg.xml file was generated correctly and can be found in following folder:"
 set path "$eWasConfigPath\\cells\\cell1\\nodes\\$node\\servers\\$webserverName"
 puts "$path"
 puts "------------------------------------------------------------"
 return -code error
} else {
 puts "------------------------------------------------------------"
 puts "Plugin propagated successfully."
 puts "------------------------------------------------------------"
}
```

2. Save the script as a text file named `plugin.jacl` in the directory:
   - Windows `<INSTALL_PATH>\eWAS\profiles\AppSrv01\bin`
   - UNIX `<INSTALL_PATH>/eWAS/profiles/AppSrv01/bin`

   The script must be run from this directory or it will not find the required files.
3. Run the script by entering: **wsadmin -f plugin.jacl.** You will be asked for the administrator username and password.

   You can verify if agents are able to connect to the administration server using the new proxy by running the tlmagent -p command on an agent that used to report to the former runtime server, which now is a proxy server. You should receive a confirmation message saying that the command has successfully executed.
4. Restart the HTTP server:
   - Windows From the **Start menu**, select **IBM HTTP server** and **Stop HTTP Server**, then **Start HTTP Server**.
   - Linux UNIX Change to the directory `/opt/IBMHttpServer` and run the apachectl stop and apachectl start commands.

The script has added a Web server, generated a plug-in, and propogated it to the remote system. The License Compliance Manager agents can now communicate with the Asset Discovery for Distributed server.

As time permits, upgrade your old License Compliance Manager agents to Asset Discovery for Distributed Version 7.2. When you have no more old agents to support, you can remove the proxy servers and re-configure agents to communicate with the Asset Discovery for Distributed server. To re-configure an agent stop it, edit the `tlmagent.ini` file to include a proper server location parameter:

```
# Preferred Server
# (Reloadable: No)
server = IP_ADDRESS
```

and start the agent.

Removing proxy definitions from WebSphere Application server (optional)

If you enabled proxy servers by installing IBM HTTP Server plug-ins in order to relay information from License Compliance Manager agents to Asset Discovery for Distributed server, you can optionally remove the proxy servers definitions in the Asset Discovery for Distributed Integrated Solutions Console after upgrading and re-configuring of all old agents. This allows you to eliminate a layer in your infrastructure and to free up resources (servers) for other purposes.

Before you begin

To remove proxy definitions from WebSphere Application server, you must have the system administrator privileges.

Note: All agents have to be re-configured to connect directly to the Asset Discovery for Distributed server before removing proxy server.

You can delete an HTTP server definition by using wsadmin commands (or by using administration console). You need to do this because the uninstaller program for the HTTP server plug-ins does not delete HTTP server definitions on the WebSphere Application Server.

To do this:

1. Log on to the Asset Discovery for Distributed server and start the server command line interface.
2. Delete a single HTTP server definition in the Tivoli Asset Discovery for Distributed server by issuing the following command:

```
$AdminTask deleteServer { -serverName webserver1 -nodeName WebserverHostName-node_node }
$AdminTask removeUnmanagedNode { -nodeName WebserverHostName-node_node }
$AdminConfig save
```

Data from agents is no longer routed through the proxy servers.

Now, you can remove the corresponding plug-in on a given IBM HTTP server and, optionally, uninstall the HTTP server to free up the computer for other purposes.

Performing post-upgrade tasks (after upgrading from Tivoli License Compliance Manager)

Perform a few tasks to finalize the upgrade and migration from Tivoli License Compliance Manager. The most important task in this group is to import customized software catalogs from Software Knowledge Base Toolkit.

Modifying the settings of Java Virtual Machine

Modify some Java Virtual Machine settings on base WebSphere Application Server to improve the scalability of your Tivoli Asset Discovery for Distributed infrastructure.

1. Open Integrated Solutions Console in your browser. The console is available at the following URL: `http://server_ip_address:9044/ibm/console`.
2. Set the Java Virtual Machine heap size.

a. In the navigation bar click **Servers** → **Application servers** and click the *server_name*.
b. In the **Configuration** tab, navigate to **Server Infrastructure** → **Java(TM) and Process Management** → **Process Definition** → **Additional Properties: Java Virtual Machine**.
c. Set the following values:

   Initial Heap Size:
   256

   Maximum Heap Size:
   1024

   Click **Apply** and then **OK**.

3. Set the thread pools size by completing the following steps:
   a. In the navigation bar click **Servers** → **Application servers** and then in the table click the *server_name*.
   b. In the **Additional Properties** section click **Thread Pools**.
   c. In the table that appears click **Default**.
   d. On the new panel supply the maximum size for thread pools:

      Maximum Size:
      100 threads

      Click **Apply** and then **OK**.
   e. Click **Web Container**. On the panel that appears supply the following value:

      Maximum Size:
      250 threads
   f. Click **Apply** and then **OK**. The Thread Pools panel appears again.
4. Save the settings and restart WebSphere Application Server.

Run scripts to install the Asset Discovery for Distributed server.

Enabling secure communication with Software Knowledge Base Toolkit

Retrieve a signer certificate from a remote Software Knowledge Base Toolkit SSL port in order to enable automatic catalog distribution between Software Knowledge Base Toolkit and Asset Discovery for Distributed. Asset Discovery for Distributed connects to the Software Knowledge Base Toolkit remote SSL port and receives the signer during the handshake using a trust manager.

Before you begin

The keystore that contains a personal certificate must already exist on the Software Knowledge Base Toolkit server.

To do this:

1. Ensure that you have configured the connection with Software Knowledge Base Toolkit. If not, do the following steps:
   a. Open the `system.properties` file. If the server is installed on the embedded version of WebSphere Application Server included in the installation package, the file is located in following directory:
      `<INSTALL_DIR>\eWAS\systemApps\isclite.ear\tad4d_admin.war\WEB-INF\conf`

If it is installed on a standalone application server, the file is located in:
`<WEBSPHERE_INSTALL_DIR>\AppServer\systemApps\isclite.ear\tad4d_admin.war\WEB-INF\conf`

b. Edit the file by specifying the software knowledge base URL. Provide the Web address in the **SwKBToolURL** parameter in the following format: `protocol_name://hostname:port/` (for example, `SwKBToolURL = https://9.156.44.150:12344/`) and restart the server.

2. In the Integrated Solutions Console left navigation bar click on **Security → SSL certificate and key management**.
3. In the SSL certificate and key management panel click on the **Key stores and certificates** link and then, in the table that opens click **NodeDefaultTrustStore**.
4. On the NodeDefaultTrustStore pane click **Signer certificates** hyperlink, which is located in the upper right-hand area of the pane. On Signer certificates pane click **Retrieve from port** button in the table header.
5. 10. Provide the connection information in order to receive the Software Knowledge Base certificate. Provide the IP address of the Software Knowledge Base Toolkitand the port number that will be used during the handshake. From the drop-down choose **3odeDefaultSSLSettings** and, in the next text field provide the Software Knowledge Base Toolkit alias. For more details regarding the parameters that need to be provided see the Retrieve from port topic in the WebSphere Application Server infocenter.
6. Click **Retrieve signer information** button. The certificate data appears. Click **Apply** and **Save**.
7. Restart the Asset Discovery for Distributed server into which you have imported the signer certificate.

When these steps are completed, the Asset Discovery for Distributed server can identify the content management server of Software Knowledge Base Toolkit as a trusted data source and enable secure import of software catalogs.

Migrating version 2.3 keystores to the Tivoli Asset Discovery for Distributed server (without external HTTP server)

If security between agents and runtime servers was configured in the previous infrastructure, you need to remember to migrate certificates to the Tivoli Asset Discovery for Distributed server before enabling the secure connection again.

Before you begin

Earlier in the upgrade process, before the runtime servers are uninstalled, copy the keystore used by the HTTP server configured for Tivoli License Compliance Manager 2.3 runtime server. To locate a path to `key.kdb`, open `httpd.conf` file and find Keyfile property in Virtual Host definitions for secure ports used to communicate with agents. The keystore can be found in the following location:

- UNIX `/opt/IBM/TLM/runtime/SLM_Runtime_Application.ear/slm_runtime.war/WEB-INF/keystore/key.kdb`
- Windows `<install_dir>\IBM\TLM\runtime\SLM_Runtime_Application.ear\slm_runtime.war\WEB-INFkeystore\key.kdb`

Store the files in a secure location or on a backup media to be used later in the upgrade process.

To do this:

1. Import the runtime server certificate from runtime keystore into Tivoli Asset Discovery for Distributed key store by performing the following steps:

a. In the Integrated Solutions Console click **SSL certificate and key management → Key stores and certificates → ILMTkeystore → Personal certificates → Import**. The Import certificates from a key file pane opens.

b. On the pane provide the following info:

Key file name:
key.kdb

Type From the dropdown list select **CMSKS**.

Key file password
Provide the password that you used to secure the key store. The default password is: **tlcm01test**.

c. Click **Get key file aliases**

Certificate alias to import
From the dropdown list select **runtime server certificate**.

Imported certificate alias
In the text field type RUNTIME_SERVER_CERTIFICATE. You can use a different alias, however, you need to provide it again when performing step 2.

d. Click **Apply** and then **OK**.

2. Replace currently used certificate with the one you have just imported. In the Integrated Solutions Console click **SSL certificate and key management → Key stores and certificates → ILMTkeystore → Personal certificates**. Select the **Alias** that you want to replace and click **Replace**. On the Replace certificate panel provide the following information and options:

Old certificate:
The name of the previous certificate. By default it is: **lmt test** certificate.

Replace with:
From the dropdown list select **RUNTIME_SERVER_CERTIFICATE**

Select the checkbox **Delete the old certificate after replacement**, click **Apply** and then **OK**.

3. If maximum security level has been defined then you need to add Certificate Authority certificate with the chain of certificates up to the root Certificate Authority certificate used to sign agent certificates to Asset Discovery for Distributed7.2 server trust store. In the Integrated Solutions Console click: **SSL certificate and key management → Key stores and certificates → ILMTtruststore → Signer certificates → Add**. On the Add signer certificate pane provide the following information:

Alias: CA (You can also provide a different alias)

File name:
cacert.pem (You can also use a different file name)

Data type:
From the dropdown list select **Base64-encoded ASCII data**

Note: A copy of Certificate Authority certificate with the chain of certificates up to the root CA certificate used to sign agent certificates can be extracted from **Signer Certificates** section of the runtime server key store `key.kdb` using IKeyMan.
Click **Apply** and then **OK**.

4. Restart the server.

Migrating version 2.3 certificates to the Tivoli Asset Discovery for Distributed server (with HTTP server on a separate machine)

If security between agents and runtime servers was configured in your previous infrastructure, you need to remember to migrate certificates to the Tivoli Asset Discovery for Distributed server before enabling the secure connection again.

Before you begin

Earlier in the upgrade process, before the runtime servers are uninstalled, copy the key store used by the HTTP server configured for Tivoli License Compliance Manager 2.3 runtime server. To locate a path to the `key.kdb` and the stash file, open the `httpd.conf` file and find Keyfile property in Virtual Host definitions for secure ports used to communicate with agents.

Store the files in a secure location or on a backup media to be used later in the upgrade process. Note down the path to the file.

Migrating certificates from the 2.3 runtime server (with reused HTTP server): Before you begin

Ensure you have correctly set up a proxy server. For detailed instructions see:

- "Configuring IBM HTTP server to forward data traffic from agents to a stand-alone WebSphere Application Server" on page 83 or
- "Configuring IBM HTTP server to forward data traffic from agents to the embedded WebSphere Application Server" on page 86

1. Copy the backed up `key.kdb` and `kdb.sth` files to the new location (outside the runtime path) and change the `httpd.conf` Keyfile directive to point to the new file.
2. Modify the plugin configuration file to enable supporting client authentication requests. Edit the `plugin-cfg.xml` file on the HTTP server. Ensure that for your WebSphere host name only one transport entry for each protocol is defined in the file:

Option	Transport entry
Insecure communication	`<Transport Hostname="WAS_HOST" Port="9988" Protocol="http"/>`

Secure communication	`<Transport Hostname="WAS_HOST" Port="9999" Protocol="https">`
	`  <Property Name="keyring" Value="/opt/IBM/HTTPServer/Plugins/config/webserver1/plugin-key.kdb"/>`
	`  <Property Name="stashfile" Value="/opt/IBM/HTTPServer/Plugins/config/webserver1/plugin-key.sth"/>`
	`</Transport>`

3. Add WebSphere Application Server certificate to the `plugin.kdb` on HTTP server.
   a. Log on to the Integrated Solutions Console.
   b. In the navigation pane, expand **Security**. Select **SSL certificate and key management → SSL configurations → ILMTsecure → Key stores and certificates** and extract the lmt server certificate, specifying the file name as: `<secure_place_on_was>/cert4ihs.arm`.
   c. Import the `cert4ihs.arm` file to the HTTP server plugin key store as a signer certificate using IKEYMAN.
4. Restart IBM HTTP server.

Migrating certificates from the 2.3 runtime server (with fresh HTTP server installation):

1. Using IKEYMAN, import the runtime server certificate from runtime server key store into Web server key store configured for Tivoli Asset Discovery for Distributed.
   a. Log on to the HTTP server and start IKEYMAN. Click **File** → **Open**.
   b. On the new dialog window provide the following information:

      Key file name:
      webserver1.kdb

      Type From the dropdown list select **CMSKS**.

      Location
      secure_place_on_ihs

      Note: In order to determine the path to `webserver1.kdb` key store used by Web server configured for Asset Discovery for Distributed, open `httpd.conf` file on the HTTP server and find key file property in Virtual Host definitions for secure ports used to communicate with agents.
   c. Click **OK**. Provide the key store password.
   d. Click **Personal certificates** and then click the button **Export/Import Key**.
   e. A new dialog window opens. Provide the following information:

      Key file type
      From the dropdown list select **CMS**.

      File name
      key.kdb

      Location
      path_to_tlcm23_keystore
   f. Provide the password that secures the source key database:

      Password to open the source key database
      tlcm01test (default)
   g. Select keys from the key list of the source key database (Remember to note down the certificate label under which you import the certificate). Click **Apply** and then **OK**.
   h. On the Change labels dialog, select a label to change. Click **OK**.
2. Configure the secure communication between the web server and the application server, keeping in mind that you need to use certificates previously present in Tivoli License Compliance Manager environment rather than create the new ones. For details see ../com.ibm.license.mgmt.security.doc/t_configuring_httpserver.dita.

Importing new catalogs

Regularly import the software catalog to keep your software inventory up-to-date.

Before you begin

- You must be assigned to the role of software asset manager or inventory administrator.
- Back up your database before importing the IBM software catalog. An unsuccessful import can cause lost or inconsistent data.

1. In the navigation bar, click **Administration** → **Import Software Catalog**.
2. You can import or upload the catalog.

- In the **Automatic Import** section, click **Import** to automatically download and import the newer version (if it exists) of the catalog from Tivoli Software Knowledge Base Toolkit to the server. Note that before importing, you have to first publish the catalog in the knowledge base.
  - You can only import the catalog when the Software Knowledge Base Toolkit application is installed in your infrastructure and its Web address is specified in `system.properties` file. If the server is installed on the embedded WebSphere Application Server included in the installation package, the file is located in following directory:

    `<INSTALL_DIR>\eWAS\systemApps\isclite.ear\tad4d_admin.war\WEB-INF\conf`

    If it is installed on a base application server, the file is located in:

    `<WEBSPHERE_INSTALL_DIR>\AppServer\systemApps\isclite.ear\tad4d_admin.war\WEB-INF\conf`

    Open the file and provide the Web address in the **SwKBToolURL** parameter in the following format: `protocol_name://hostname:port/` (for example, `SwKBToolURL = https://9.156.44.150:12344/`). Restart the server.

  The Importing Software Catalog window opens. You can view there the status of import process.

  Tip: The status is refreshed by default every 10 seconds. However, you can change the default value in **Settings** → **Manage Global Refresh**, or you can manually refresh the progress bar by clicking  , and choosing **Manual Refresh**.
- Manually import the catalog from the knowledge base by clicking the **Software Knowledge Base Toolkit** link. To upload the catalog from your computer, in the **Manual Import** section, click **Browse**, select the file (in XML or ZIP format), and click **Upload**.

You have to wait some time to verify the changes (approximately up to 60 minutes).

Verifying the server installation

Check the log files and start the Web user interface to verify that the server installation has been successful.

The log files together with the Web interface, also called the Integrated Solutions Console, contain information that will allow you to check if the application server has been successfully installed. You can access the Web interface using most of the common Web browsers.

Note: It is important not to turn the JavaScript option off in your browser, as some of the functionalities of the Web interface might not function properly.

1. Open the `msg_servers.log` file and check if it contains information that the application was successfully installed. The file is by default stored under the following path: `<Tivoli_Common_Directory>/COD/logs/install/message`.
2. Access the login page at the following address: `http://`*`administration_server_IP_address`*`:8899/ibm/console/login.do` and check the Home page for information about any problems that might have occurred during installation.

   If the application is deployed on a base WebSphere Application Server, the port number is specific for the profile.

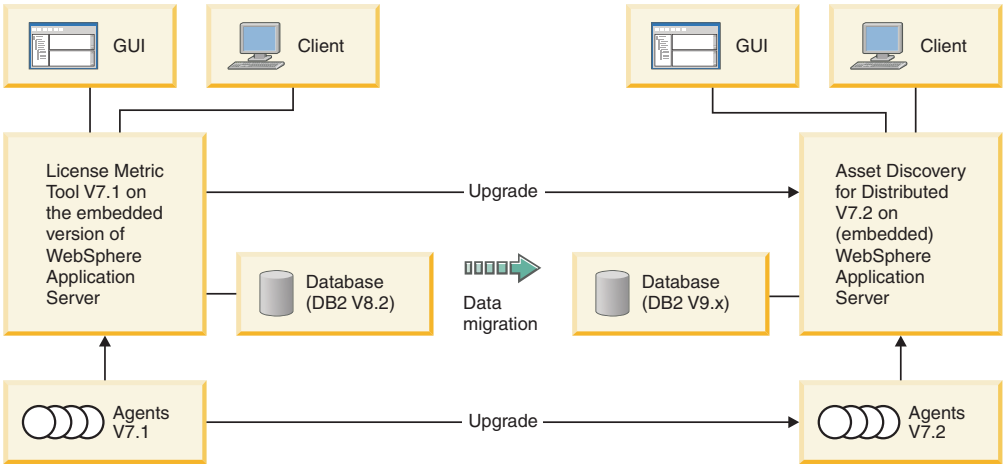
- Windows On Windows platforms, you can also open the login page from the system Start menu.

3. Click **OK**. You do not need to provide any credentials at this stage.

Upgrading from IBM License Metric Tool 7.1 to Tivoli Asset Discovery for Distributed 7.2

Upgrade your License Metric Tool 7.1 instance to Tivoli Asset Discovery for Distributed 7.2.

IBM License Metric Tool includes the following physical components that form the basis of the monitoring infrastructure: an administration server consisting of a DB2 database and Web interface, and agents that run on computers where IBM software is installed. The diagram below shows you the upgrade procedure for each of the components.



To upgrade the product, you need to upgrade all of its components. It is recommended to upgrade the server first before upgrading the agents to be able to run the product under this latest version.

To upgrade to Tivoli Asset Discovery for Distributed, perform the following tasks:

1. Prepare to upgrade.
2. Choose the installation method:
   - Upgrade interactively on the embedded version of IBM WebSphere Application Server. This upgrade method is suitable for small to medium-sized environments (up to 5000 agents per server). It uses the installation wizard.
   - Upgrade in silent mode on the embedded version of IBM WebSphere Application Server. In this method, the upgrade installer takes the necessary parameters from the response file so that the upgrade process runs without your interaction.
   - Upgrade on the stand-alone version of IBM WebSphere Application Server. This method is suitable for larger environments and allows you to deploy a greater number of agents (up to 45000).
3. Upgrade agents.

Upgrading the IBM License Metric Tool 7.1 server components to Tivoli Asset Discovery for Distributed 7.2 on the embedded version of IBM WebSphere Application Server

Upgrade IBM License Metric Tool 7.1 to Tivoli Asset Discovery for Distributed 7.2 on the embedded version of IBM WebSphere Application server using the upgrade wizard on distributed operating system platforms.

Before you begin

Ensure that you have completed all the pre-upgrade tasks described in "Preparing to upgrade" on page 100

- You must have the following operating system privileges:
  - Windows Administrator
  - UNIX root
- You require a valid DB2 administrator ID.

Asset Discovery for Distributed server is a solution that consists of an administrative server, database and agents. The launchpad is the single point of reference for upgrading the entire server environment.

To do this:

1. If you are upgrading in distributed environment, stop the server by running the <application_folder_location>/cli/srvstop.sh command. The <*application_folder_location*> is either the full or relative path to the folder where License Metric Tool is located.
2. Start the Tivoli Asset Discovery for Distributed launchpad from the root directory of the product disk or the downloaded installation image by clicking **launchpad.exe** (Windows) or **launchpad.sh** (other platforms). If you are upgrading in distributed environment, you should start the launchpad on the machine where the database is installed. The launchpad detects and upgrades it.
3. Launch the installation wizard by clicking **Install** and **Launch the server installation or upgrade wizard**.
4. Accept the license and click **Next**.
5. Enter the `tlmsrv` user password.
6. Review the installation information and ensure that you have enough space to complete the upgrade. When the upgrade process completes successfully, a summary panel opens.
7. If you are upgrading in distributed environment, you should start the launchpad on the machine where the server is installed and repeat steps 2 to 6.

You have upgraded the IBM License Metric Tool 7.1 server components to Tivoli Asset Discovery for Distributed 7.2.

Apply the following fix packs:

- embedded WebSphere Application Server, version 6.1.0 fix pack 23
- Integrated Solutions Console, version 7.1.0, fix pack 7.

To apply the fix packs, you need to download Update Installer from the WebSphere Application Server Web page: http://www-01.ibm.com/support/docview.wss?rs=180&uid=swg24012718. Fix pack 23 can be downloaded from the following location:

ftp://ftp.software.ibm.com/software/websphere/appserv/support/fixpacks/was61/cumulative/cf61023/

The file 6.1.0.11-WS-WASFeature-FEISCAE7107EWAS.pak is available in the following directory on the DVD or the package downloaded from Passport Advantage: server/fixpacks.

- Verify that the product upgraded successfully by logging into the Integrated Solutions Console and checking if Tivoli Asset Discovery for Distributed 7.2 appears in the navigation bar.

Upgrading the IBM License Metric Tool 7.1 server to Tivoli Asset Discovery for Distributed 7.2 in silent mode

Specify the requisite upgrade parameters by editing the response file before upgrade to upgrade in silent mode. The installer takes the necessary parameters from the response file (response_file.txt) and the upgrade process runs without your interaction.

Before you begin

To run the upgrade in silent mode, you need to log in to your system with rights that will enable you to edit and save the response file. For more information about response file parameters, see Server installation and upgrade response files.

If you are upgrading in distributed environment, stop the server by running the <application_folder_location>/cli/srvstop.sh command. The <*application_folder_location*> is either the full or relative path to the folder where License Metric Tool is located.

To run the upgrade wizard in silent mode, perform the following tasks:

1. Log on to the computer where you want to install the server and the database components as a user with administrative rights (Administrator on Windows platforms or root on other platforms).
2. Copy the response file from the product DVD to a temporary directory on your hard disk. The response file is located in the Server subdirectory of the Launchpad directory.
3. Update the response file with the parameters for the upgrade that you want to perform and save the file. The file has been enhanced by two parameters that you need to specify before starting the upgrade process:

   -W credentials.adminUser="was1"
   -W credentials.adminPassword="abc12def"
   Specifies WebSphere Application Server user ID and password. This parameter is required only if the WebSphere Application Server cell is in security mode.

   -W credentials.adminDBUser="tlmsrv"
   -W credentials.adminDBPassword="abc12def"
   Specifies database server user ID and password. This parameter is required only if the database is being upgraded. The default user value is tlmsrv.

   Read and agree with the license terms that are provided in the license.txt file located in one of the subdirectories of the license directory on the product DVD and uncomment the appropriate line in the response file.
4. Run the following command to start silent upgrade:
   - TAD4D-server-7.2-<platform>.bat -options <response_file_path> -silent (Windows)

- TAD4D-server-7.2-<platform>.sh -options <response_file_path> -silent (other platforms)

  The <*response_file_path*> is either the full or relative path to the response file that you are using.

The upgrade process runs in the background. When it is finished, a message informing you that the upgrade was successful will be recorded in the logs.

Verify that the program was upgraded successfully by logging into the Integrated Solutions Console (`http://administration server IP address:8899/ibm/console/login.do`) and checking if Tivoli Asset Discovery for Distributed 7.2 version appears.

Upgrading IBM License Metric Tool 7.1 to Tivoli Asset Discovery for Distributed 7.2 on the stand-alone version of WebSphere Application Server

Upgrade License Metric Tool 7.1 to Asset Discovery for Distributed 7.2 on the stand-alone version of WebSphere Application Server. This method allows you to deploy a greater number of agents in your infrastructure (up to 45000) and is suitable for larger environments.

Before you begin

Ensure that you have performed all the pre-upgrade tasks described in "Preparing to upgrade" on page 100.

You must have the following operating system privileges:

- Windows Administrator
- UNIX root

You require a valid DB2 administrator ID.

Important: The scripts used in this method are only sample scripts. Before using them, check if they meet your requirements and modify them, if necessary.

1. Uninstall the License Metric Tool 7.1 server:

   UNIX On Unix platforms:

   a. Run the <application_folder_location>/cli/srvstop.sh command to stop the server.
   b. Run the <application_folder_location>/_uninst/uninstaller.bin command to uninstall the server.

   The <*application_folder_location*> is either the full or relative path to the folder where License Metric Tool is located.

   Windows On Windows:

   a. Open the directory *INSTALL_DIR*`/cli`, where *INSTALL_DIR* is the name of the installation directory. Run the srvstop.bat command to stop the server.
   b. Select the **Add/Remove Programs** option from the **Control Panel**.
   c. Click on License Metric Tool and then on **Remove** or **Change/Remove**, whichever is displayed.

   Follow the instructions on the panels to uninstall the server. Remember to deselect the database, which should not be uninstalled. When the uninstallation is complete, click **Finish** to exit from the wizard.

2. Install WebSphere Application Server, version 6.1 on the machine where you want to install the server. For more information on how to do it, visit WebSphere Application Server information center: http://publib.boulder.ibm.com/infocenter/wasinfo/v6r1/topic/com.ibm.websphere.nd.multiplatform.doc/info/ae/ae/welc6topinstalling.html.
3. Upgrade the database:
   a. On the machine where the database is installed, launch the installation wizard by clicking **Install** and **Launch the server installation or upgrade wizard**. The license acceptance panel opens.
   b. Accept the licence and click **Next**.
   c. Enter the `tlmsrv` user password.
   d. Review the installation information and ensure that you have enough space to complete the upgrade. When the upgrade process completes successfully, a summary panel opens.
4. Install the Asset Discovery for Distributed 7.2 server on the stand-alone version of WebSphere Application Server. For more information on how to do it, see Installing the Tivoli Asset Discovery for Distributed on WebSphere Application Server.
5. Upgrade agents.

You have successfully upgraded the License Metric Tool 7.1 server and database.

Verify that the program was upgraded successfully by logging into the Integrated Solutions Console (`http://administration server IP address:portNumber/ibm/console/login.do`) and checking if Tivoli Asset Discovery for Distributed 7.2 appears in the navigation bar.

Preparing to upgrade

Before upgrading the product, you need to review all of the applicable upgrade prerequisites and pre-upgrade tasks to ensure that the upgrade proceeds smoothly.

Before you begin

The License Metric Tool V7.1 server with security level set to Medium is able to communicate with agents with security set to Minimum. Bear in mind that after upgrading License Metric Tool 7.1 to Tivoli Asset Discovery for Distributed V7.2 it is no longer possible because the server manages the agents only with the same or higher level of security.

Ensure that you have done the following pre-upgrade tasks:

1. Sign all the IBM reports as close to the date of the upgrade as possible to limit the amount of data from the reports that will be recalculated. After migrating the data to Tivoli Asset Discovery for Distributed V7.2 the recalculation process will recalculate all data starting from the first day after last signed report. If the amount of data is big, you may experience performance problems because the server will be fully occupied with data recalculation. The reports that are only partially in the signed period will be deleted. The version of the reports with end date before or on the last signed date will be set to 7.1.
2. Check what version of the database you are using. Tivoli Asset Discovery for Distributed supports DB2 version 9.1 or higher so if you are using a lower version of the database, you will need to upgrade it to version 9.1 or higher before upgrading the server. To find out how to do it, refer to DB2 Information Center: http://publib.boulder.ibm.com/infocenter/db2luw/v9/index.jsp.

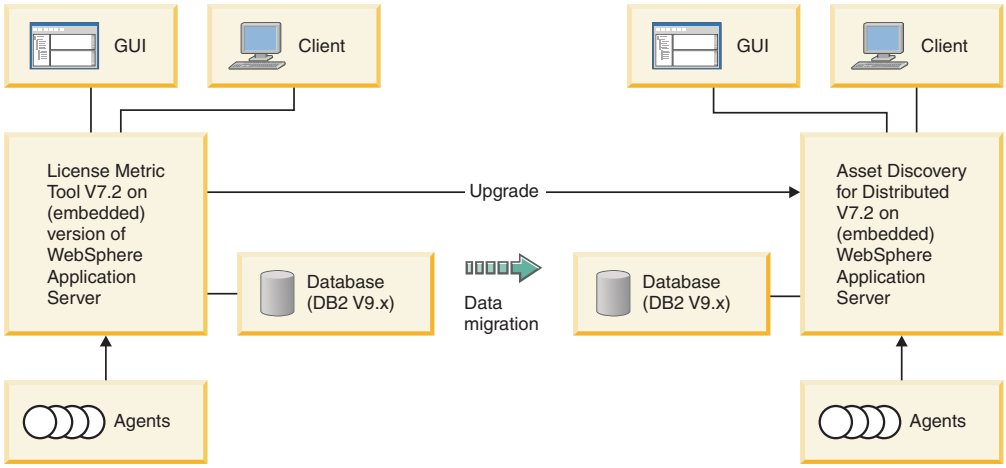
3. If you are installing on the stand-alone version of WebSphere Application Server, ensure that WebSphere Application Server, fix pack 23 and Integrated Solutions Console, version 7.1.0.7 or higher are installed on the machine where you want to perform the upgrade.
4. If you have enabled secure agent-server communication and your target environment is based on the stand-alone version of WebSphere Application Server, you need to export server and agent certificates for License Metric Tool. After you have exported the certificates, import them to the WebSphere Application Server keystore.
5. (Recommended) Back up your database and the directory. This way you will be able to recover it in case an error during the upgrade process occurs. To find out how to back up the database, refer to DB2 Information Center: http://publib.boulder.ibm.com/infocenter/db2luw/v9/index.jsp. If you perform the back up of the directory, ensure that you retain your rights to the application files.

Note: To upgrade your product to this latest version, you do not need to have either of the Fix Packs installed.

Upgrading from IBM License Metric Tool 7.2 to Tivoli Asset Discovery for Distributed 7.2

Upgrade your License Metric Tool 7.2 instance to Tivoli Asset Discovery for Distributed 7.2

License Metric Tool includes the following physical components that form the basis of the monitoring infrastructure: an administration server consisting of a DB2 database and Web interface, and agents that run on computer where IBM software is installed. The diagram below shows you the structure of Tivoli Asset Discovery for Distributed 7.2 and the upgrade procedure of each of the product components.



To upgrade the product, you need to upgrade only the server. There is no need to upgrade the agents because the License Metric Tool V7.2 agents are the same ones that Tivoli Asset Discovery for Distributed uses.

To upgrade to Tivoli Asset Discovery for Distributed 7.2, perform the following tasks:

1. (Recommended) Back up your database. This way you will be able to recover it in case an error during the upgrade process occurs. To find out how to back up the database, refer to DB2 Information Center: http://publib.boulder.ibm.com/infocenter/db2luw/v9/index.jsp.
2. Choose the installation method:
   - Upgrade interactively on the embedded version of IBM WebSphere Application Server. This upgrade method is suitable for small to medium-sized environments (up to 5000 agents per server). It uses the installation wizard.
   - Upgrade in silent mode on the embedded version of IBM WebSphere Application Server. In this method, the upgrade installer takes the necessary parameters from the response file so that the upgrade process runs without your interaction.
   - Upgrade on the stand-alone version of IBM WebSphere Application Server. This method allows you to deploy a greater number of agents in your infrastructure (up to 45000) and is suitable for complex and more complicated topologies.
3. There is no need to upgrade the agents. After the agents download new parameters from the server, they will offer new, Asset Discovery for Distributed functionalities.

Upgrading the IBM License Metric Tool 7.2 server components to Tivoli Asset Discovery for Distributed 7.2 on the embedded version of IBM WebSphere Application Server

Upgrade IBM License Metric Tool 7.2 to Tivoli Asset Discovery for Distributed 7.2 on the embedded version of the IBM WebSphere Application Server using the upgrade wizard on distributed operating system platforms.

Before you begin

- You must have the following operating system privileges:
  - Windows Administrator
  - UNIX root
- You require valid credentials for the **tlmsrv** DB2 user.

Tivoli Asset Discovery for Distributed is a solution that consists of an administrative server, database and agents. The launchpad is the single point of reference for upgrading the entire server environment.

1. If you are upgrading in distributed environment, stop the server by running the <application_folder_location>/cli/srvstop.sh command. The *<application_folder_location>* is either the full or relative path to the folder where License Metric Tool is located.
2. Start the Tivoli Asset Discovery for Distributed launchpad from the root directory of the product disk or the downloaded installation image by clicking **launchpad.exe** (Windows) or **launchpad.sh** (other platforms). If you are upgrading in distributed environment, you should start the launchpad on the machine where the database is installed.
3. Launch the installation wizard by clicking **Install** and **Launch the server installation or upgrade wizard**. The license acceptance panel opens.
4. Accept the license and click **Next**.
5. Enter the `tlmsrv` user password.

6. Review the installation information and ensure that you have enough space to complete the upgrade. When the upgrade process completes successfully, a summary panel opens.
7. If you are upgrading in distributed environment, you should now start the launchpad on the machine where the server is installed and repeat steps 2 to 6.

You have upgraded the IBM License Metric Tool 7.2 server components to Tivoli Asset Discovery for Distributed 7.2.

Verify that the product upgraded successfully by logging into the Integrated Solutions Console (`http://administration server IP address:8899/ibm/console/login.do`) and checking if Tivoli Asset Discovery for Distributed 7.2 appears in the navigation bar.

Upgrading the IBM License Metric Tool 7.2 server to Tivoli Asset Discovery for Distributed 7.2 in silent mode

Specify the requisite upgrade parameters by editing the response file before upgrade to upgrade in silent mode. The installer takes the necessary parameters from the response file (`response_file.txt`) and the upgrade process runs without your interaction.

Before you begin

To run the upgrade in silent mode, you need to log in to your system with rights that will enable you to edit and save the response file. For more information about response file parameters, see Server installation and upgrade response files.

To run the upgrade wizard in silent mode, perform the following tasks:

1. If you are upgrading in distributed environment, stop the server by running the <application_folder_location>/cli/srvstop.sh command. The `<application_folder_location>` is either the full or relative path to the folder where License Metric Tool is located
2. Log on to the computer where the V7.2 License Metric Tool server and the database components are installed as a user with administrative rights (Administrator on Windows platforms or root on other platforms). If you are upgrading in distributed environment, you should first log in to the machine where the database is installed.
3. Copy the response file from the product DVD to a temporary directory on your hard disk. The response file is located in the `Server` subdirectory of the `Launchpad` directory.
4. Update the response file with the parameters for the upgrade that you want to perform and save the file. The file has been enhanced by our parameters that you need to specify before starting the upgrade process:

   -W credentials.adminUser="was1"
   -W credentials.adminPassword="abc12def"
   Specifies WebSphere Application Server user ID and password. This parameter is required only if the WebSphere Application Server cell is in security mode.

   -W credentials.adminDBUser="tlmsrv"
   -W credentials.adminDBPassword="abc12def"
   Specifies database server user ID and password. This parameter is required only if the database is being upgraded. The default user value is tlmsrv.

Read and agree with the license terms that are provided in the `license.txt` file located in one of the subdirectories of the `license` directory on the product DVD and uncomment the appropriate line in the response file.

5. If you are upgrading in distributed environment, stop the server by running the <application_folder_location>/cli/srvstop.sh command. The *<application_folder_location>* is either the full or relative path to the folder where License Metric Tool is located.
6. Run the following command to start silent upgrade:
   - TAD4D-server-7.2-<platform>.bat -options <reponse_file_path> -silent (Windows)
   - TAD4D-server-7.2-<platform>.sh -options <reponse_file_path> -silent (other platforms)

   The *<response_file>* is either the full or relative path to the response file that you are using.
7. If you are upgrading in distributed environment, you should now repeat the steps 2 to 5 on the computer where the server is installed.

The upgrade runs in the background. When it is finished, you will receive a message informing you that the upgrade was successful.

Verify that the program was upgraded successfully by logging into the Integrated Solutions Console (`http://administration server IP address:8899/ibm/console/login.do`) and checking if Tivoli Asset Discovery for Distributed 7.2 appears in the navigation bar.

Upgrading IBM License Metric Tool 7.2 to Tivoli Asset Discovery for Distributed 7.2 on the stand-alone version of IBM WebSphere Application Server

Upgrade License Metric Tool 7.2 to Tivoli Asset Discovery for Distributed 7.2 on the stand-alone version of IBM WebSphere Application server. This method allows you to deploy a greater number of agents in your infrastructure (up to 45000) and is suitable for larger environments.

Before you begin

- Ensure that WebSphere Application Server, fix pack 23 and Integrated Solutions Console, version 7.1.0.7 or higher are installed on the machine where you want to perform the upgrade. The same requirements need to be fulfilled for License Metric Tool 7.2, so if you are upgrading from it, both products should be already installed on your machine.
- If you are upgrading in distributed environment, stop the server by running the <application_folder_location>/cli/srvstop.sh command. The *<application_folder_location>* is either the full or relative path to the folder where License Metric Tool is located.
- Clean up the settings that you have applied to License Metric Tool 7.2 and delete the old applications from the server to ensure that the upgrade runs smoothly. To do this, you need to perform the following steps:

Important: The scripts used in this method are only sample scripts. Before using them, check if they meet your requirements and modify them, if necessary.

1. Clean up your environment.
2. Extract the installation files.
3. Migrate the contents of the administration server database.

4. Edit the properties file.
5. Install the server components.

You have successfully upgraded the server and its components.

Verify that the program was upgraded successfully by logging into the Integrated Solutions Console (`http://administration server IP address:8899/ibm/console/login.do`) and checking if Tivoli Asset Discovery for Distributed 7.2 appears in the navigation bar.

Cleaning up your environment before upgrading to Tivoli Asset Discovery for Distributed 7.2

Clean up the settings that you have applied to License Metric Tool 7.2 and delete the old applications from the server to ensure that the upgrade runs smoothly.

Perform the following steps:

1. Edit the `setupWAS.properties` file. Use the same parameter values that you used during License Metric Tool 7.2 installation.
2. Run the `cleanupWAS.bat` script.
3. Restart the server.
4. Remove the `tad4d_admin.war` file from the `isclite.ear` directory in the WebSphere installation folder.

Now you can move on to upgrading the server.

Extracting the installation files from the interactive installer

Use the Asset Discovery for Distributed installation wizard to extract the files needed for upgrading the server and command-line interface.

Before you begin

Ensure that you have created and augmented the Asset Discovery for Distributed WebSphere Application Server profile.

To do this task:

1. Run **launchpad.exe** (Windows) or **launchpad.sh** (other platforms). The Welcome page opens.
2. In the left-hand navigation pane, click **Install or upgrade to Tivoli Asset Discovery for Distributed**.
3. Click **Launch the server installation wizard**.
4. Select the language of the installation and click **OK**. The installation wizard starts.
5. Click **Next**. After accepting the license agreement, click **Next** again.
6. Select **Production Environment** as the type of installation and proceed to the next page. This page opens only if no previous version of the product is discovered in the system.
7. On next panel select the **Unpack the files needed for manual deployment** option and specify the directory where you want to extract the files and click **Next**.
8. Specify the directory where you want to extract the files and click **Next**.
9. A progress indicator shows when the extract is complete. Click **Finish**.

The installer extracts the required installation files, including the keystore files `key.p12` and `trust.jks`, needed to enable secure communications between the server and its agents.

Note: If you enabled security before performing the upgrade, you should obtain the keystore files from the existing runtime installation.

The installation package contains the installation files, keystore files, JDBC driver files and the command-line interface. You can delete the .ear and .war installation files after you have deployed them. However, you must retain keystore files, JDBC driver files and the command-line interface files. It is recommended that you move them to the Asset Discovery for Distributed installation directory for easy reference.

Migrating the contents of the administration server database

Use the installation wizard to migrate the contents of the IBM License Metric Tool 7.2 administration server database to the Tivoli Asset Discovery for Distributed 7.2 database.

Before you begin

- You must have a valid DB2 administrator ID.
- You should back up the administration database. This way you will be able to recover it in case an error during the upgrade process occurs. To find out how to back up the database, refer to DB2 Information Center: http://publib.boulder.ibm.com/infocenter/db2luw/v9/index.jsp.

When upgrading on WebSphere Application Server, you need to migrate the contents of the database to Tivoli Asset Discovery for Distributed database format before deploying Tivoli Asset Discovery for Distributed 7.2. You can do it using the launchpad.

1. Log in with the following privileges:
   - Windows Administrator
   - UNIX root
2. Start the Tivoli Asset Discovery for Distributed launchpad from the root directory of the product disk or the downloaded installation image by clicking **launchpad.exe** (Windows) or **launchpad.sh** (other platforms).
3. Launch the installation wizard by clicking **Install** and **Launch the server installation or upgrade wizard**. The license acceptance panel opens.
4. Accept the license and click **Next**.
5. Select **Production Environment** as the type of installation.
6. Accept the default installation location or click **Browse** to select a different location. Click **Next**
7. Select **Administration server database** as the component that you want to install. Confirm your choice.
8. Select **Locate the DB2 directory** and specify the path to the existing DB2 installation directory.
9. Connect to the administration server database by entering the password for the existing `tlmsrv` user. Click **Next**. The installation wizard will detect the existing TLMA database and inform you that it will be migrated to 7.2.0.0.
10. If more than one customer is defined in the database, select the one that you want to migrate and the scan group that you want to make default. If you set the minimum or medium security level, agents can communicate with the

server by either the secure or the unsecure port, depending on the security level defined when the agent is deployed. If you set the maximum security level, when you deploy agents you must set the same level of security for all agents that are to contact the server.

11. Check the information about the installation and ensure that you have enough space to complete the process, then click **Next**. When the installation completes successfully, a summary page opens.

You have migrated the contents of License Metric Tool 7.2 database to Tivoli Asset Discovery for Distributed 7.2.

Now you can upgrade the server.

Editing the SetupWAS.properties file

Before deploying the Tivoli Asset Discovery for Distributed server, edit the SetupWAS.properties file to reflect your hardware and infrastructure. To ensure the success of your deployment, it is important to provide accurate data in this file.

Before you begin

You need to collect the configuration and security information about your WebSphere Application Server installation that is described in the following steps.

You will also need the database deployment details such as host name or IP address of the machine where DB2 is installed, database port number, user name and password.

Provide the following information in the `Setup.properties` file by performing the following steps:

1. Open the `SetupWAS.properties` file in a text editor.
2. Specify all of the following values:
   a. Name of WebSphere Application Server cell and server node.
      Example: **cellName=***nc044112Node01Cell*
      Example: **nodeName=***nc044112Node01*

      Tip: You can obtain the cell name and the node name from the name of your WebSphere Application server profile. For example, if your profile is Windows `C:\Program Files\IBM\WebSphere\AppServer\profiles\AppSrv01\config\cells\nc044184Node01Cell\nodes\nc044184Node01\`, the *nc044184Node01Cell* value is the name of the cell, and the *nc044184Node01* is the name of the node.
   b. Name of WebSphere Application Server server.
      Example: **serverName=***server1*
      server1 is the default server.
   c. WebSphere Application Server installation directory. Example:
      - Windows **wasHome=**`C:/Program Files/IBM/WebSphere/AppServer`
      - UNIX **wasHome=**`/opt/IBM/WebSphere/AppServer`
   d. Path to the directory that contains the admin package (`tad4d_admin.war`).
   e. Path to the directory that contains `com.ibm.license.mgmt.msghandler.ear` package.
   f. Domain name or IP address of the host, where the database is installed.

Example: **dbHostName=***localhost*

g. Database port number.

Example: **dbPortNumber=***50000*

h. Name of database user.

Example: **dbUser=***tlmsrv*

tlmsrv is the default user name in Tivoli License Compliance Manager.

i. Password for the database user. (Specify temporarily and delete after deployment or provide during installation when a pop-up window appears).

Example: **dbPassword=***xxxxxxx*

j. Full path to keystore files `key.p12`, `trust.jks`.

For information on how to prepare the keystore files see the *Security* section of the information center.

k. Port for minimum security level transport:

Default: **minSecurityPort=***9988*

l. Port for medium security level transport:

Default: **minSecurityPort=***9999*

m. Port for maximum security level transport:

Default: **minSecurityPort=***9977*

3. Save the file.

Installing the server components

After extracting the installation files and editing the SetupWAS.properties file, you are ready to install the Asset Discovery for Distributed server by running the scripts that you extracted.

Before you begin

Important: The scripts used in this method are only sample scripts. Before using them, check if they meet your requirements and modify them, if necessary.

Tip: If security is enabled on the WebSphere Application Server, you can specify your user name and password in the `soap.client.props` file in the properties directory of your WebSphere Application Server profile. To avoid any security risks, you can then additionally encrypt the file using the **PropFilePasswordEncoder** utility. See the WebSphere Application Server information center for more information.

To do this:

1. Copy the files `com.ibm.license.mgmt.msghandler.ear` and `tad4d_admin.war`, and the directory `WAS-scripts` from the directory where you extracted the installation files to the computer where WebSphere Application Server is installed. The directory `WAS-scripts` contains the following scripts:

   installAdmin.jacl
   Installs the administration component.

   installMessageHandler.jacl
   Installs the Message Handler component.

   setupDataSources.jacl
   Configures Data Sources and data base authentication.

   setupTimerManager.jacl
   Configures Timer Managers.

setupTivoliCommonDir.jacl
Configures Tivoli Common Directory.

setupServerSecurePorts.jacl
Configures the communication between the server and agents.

setupWebContainer.jacl
Sets up the Web container (for WebSphere Application server?).

2. Open a system command prompt and run the following command:
   - Windows **setupWAS.bat** *PATH_TO_WAS_PROFILE_DIRECTORY* [-log log_file_path]

     Note: On Windows, the path to the WAS profile directory should be provided within double quotation marks.

     An example of profile_path:

     ```
     ./setupWAS.bat "C:/Program Files/IBM/WebSphere/AppServer/profiles/
     AppSrv01"
     ```
   - Linux UNIX **setupWAS.sh** *PATH_TO_WAS_PROFILE_DIRECTORY* [-l log log_file_path]

   where *PATH_TO_WAS_PROFILE_DIRECTORY* is the path to the WebSphere Application Server profile directory.

   An example of profile_path:

   `./setupWAS.sh /opt/IBM/WebSphere/AppServer/profiles/AppSrv01/`If you do not specify the log file, the default `SetupWAS.log` file will be used. The scripts may take a few minutes to finish.
3. Restart WebSphere Application Server.

Enable the command-line interface.

Cleaning up your environment before upgrading to Tivoli Asset Discovery for Distributed 7.2

Clean up the settings that you have applied to License Metric Tool 7.2 and delete the old applications from the server to ensure that the upgrade runs smoothly.

Perform the following steps:

1. Edit the `setupWAS.properties` file. Use the same parameter values that you used during License Metric Tool 7.2 installation.
2. Run the `cleanupWAS.bat` script.
3. Restart the server.
4. Remove the `tad4d_admin.war` file from the `isclite.ear` directory in the WebSphere installation folder.

Now you can move on to upgrading the server.

Migrating the contents of the administration server database

Use the installation wizard to migrate the contents of the IBM License Metric Tool 7.2 administration server database to the Tivoli Asset Discovery for Distributed 7.2 database.

Before you begin

- You must have a valid DB2 administrator ID.

- You should back up the administration database. This way you will be able to recover it in case an error during the upgrade process occurs. To find out how to back up the database, refer to DB2 Information Center: http://publib.boulder.ibm.com/infocenter/db2luw/v9/index.jsp.

When upgrading on WebSphere Application Server, you need to migrate the contents of the database to Tivoli Asset Discovery for Distributed database format before deploying Tivoli Asset Discovery for Distributed 7.2. You can do it using the launchpad.

1. Log in with the following privileges:
   - Windows Administrator
   - UNIX root
2. Start the Tivoli Asset Discovery for Distributed launchpad from the root directory of the product disk or the downloaded installation image by clicking **launchpad.exe** (Windows) or **launchpad.sh** (other platforms).
3. Launch the installation wizard by clicking **Install** and **Launch the server installation or upgrade wizard**. The license acceptance panel opens.
4. Accept the license and click **Next**.
5. Select **Production Environment** as the type of installation.
6. Accept the default installation location or click **Browse** to select a different location. Click **Next**
7. Select **Administration server database** as the component that you want to install. Confirm your choice.
8. Select **Locate the DB2 directory** and specify the path to the existing DB2 installation directory.
9. Connect to the administration server database by entering the password for the existing `tlmsrv` user. Click **Next**. The installation wizard will detect the existing TLMA database and inform you that it will be migrated to 7.2.0.0.
10. If more than one customer is defined in the database, select the one that you want to migrate and the scan group that you want to make default. If you set the minimum or medium security level, agents can communicate with the server by either the secure or the unsecure port, depending on the security level defined when the agent is deployed. If you set the maximum security level, when you deploy agents you must set the same level of security for all agents that are to contact the server.
11. Check the information about the installation and ensure that you have enough space to complete the process, then click **Next**. When the installation completes successfully, a summary page opens.

You have migrated the contents of License Metric Tool 7.2 database to Tivoli Asset Discovery for Distributed 7.2.

Now you can upgrade the server.

Upgrading agents

After you have upgraded and configured the server, you can upgrade the agents.

Tivoli Asset Discovery for Distributed provides several methods for upgrading the agents on the computers that you want to monitor. You can use the native installation tools for your operating system, or, in environments where IBM Tivoli Configuration Manager is implemented, upgrade the agents in bulk using its

software distribution functions. On Windows platforms, you can also upgrade the agents using logon scripts. There is also a possibility to upgrade agents using the self-update method.

Note: Data which has not been uploaded to the server and which is stored in agent cache will be deleted during agent upgrade. To avoid data loss, perform a manual call using agent command line interface prior to upgrading an agent. You need to issue the command tlmagent -hw.

1. Ensure that the machine where you are upgrading the agent fulfills all hardware and software requirements.
2. Prepare the following information:
   - Level of security that has been configured for the server. For medium or maximum security levels, you will also need to prepare your own SSL certificate.
   - If you want the agent to use a proxy server for communication with the server, you also need to provide the proxy port and address.
3. Configure any firewalls between the agent and server machines to allow the agent access to the server.
4. If Windows Terminal Server is installed on the computer where you want to run the setup file, or you are accessing another computer using Windows Terminal Services, ensure that the computer is in install mode when the setup file is launched.
   a. Issue the command `change user /install` from a Windows command line to change into install mode manually.
   b. Run the setup file.
   c. Issue the command `change user /execute` to return to execute mode after the installation has completed.
5. If you are upgrading the agent in a partitioned environment using VMware or Microsoft Virtual Server virtualization technologies, check if the machine can be connected to a virtual machine manager.

   If your machine cannot be connected to a VM manager, run the Common Inventory Technology enabler.
6. Red Hat If you are upgrading on RedHat Linux, set SELinux to disabled.
7. Upgrade the agents. Depending on your platform, you can choose one of the following actions:
   - Upgrade the agents using the native installers for your platform. This method is available for all supported platforms. However, response files are not used during the upgrade process. The configuration changes that are needed must be applied after the upgrade is performed.
   - Use IBM Tivoli Configuration Manager to upgrade the agents in bulk. This method is available for all supported platforms, for environments where Configuration Manager is installed.
   - Windows Upgrade the agents using Windows logon scripts. This method is available for Windows platforms.
   - Use the automatic agent self-update facility to apply upgrades to the agents or to any of its corequisites.
8. To verify that the upgrade was successful, check if the agents appear in the Web interface of the server.

Adding scan groups

To organize scan schedules, first create scan groups and then associate agents with those scan groups.

The agents belonging to the same scan group share the same configuration parameters, for example the same scan schedule, set by means of the setagentconf command or by means of the user interface.

Before you begin

 You must be an inventory administrator to perform this task.

1. In the navigation bar, click **Infrastructure** → **Scan Groups**.
2. From the **Select Action** list, choose **Add Scan Group**, and click **Go**. The Add Scan Group window opens.
3. Enter a descriptive name for the agents that you will associate with the scan group. For example, if you plan to scan all computers in the same business unit according to the same schedule, name the scan group after the business unit, such as `Asia/Pacific region`.

   Tip: You will still be able to modify the name of a given scan group in the future.
4. In the **Set Software Scan Schedule** section, specify when you want to scan the computers in this group by filling in the **Date** and **Time** fields.
5. Specify whether you want to repeat the scan or run it only once by selecting appropriate radio button. For example, you might scan the computers once per week, starting next Saturday at 12 midnight. Note that the default software scan frequency is one week, the maximum is 9999 months, and the minimum is 1 day.
6. Select the **Enable hardware scan** check box to schedule hardware scans for this group, and provide the date and time when you want to initiate the hardware scan and its frequency. Note that the default hardware scan frequency is once a month, the maximum is 9999 months, and the minimum is 1 day.

   Note: Tivoli Asset Discovery for Distributed features the hardware inventory collection feature. It consists of an additional scan that is responsible for collecting hardware information related to, for example, printers, USB devices, or video cards. Hardware scan is enabled by default.
7. To save the scan group, click **OK**.

Now you can install agents and associate them with the new scan group. You can also reassign agents from another scan group to this scan group, for example the one that is marked as default, to this scan group.

Running Common Inventory Technology enabler

You must run the Common Inventory Technology enabler before installing Tivoli Asset Discovery for Distributed agents on any hosts with guest operating systems that run either under Microsoft Virtual Server or a VMware server that does not use the VMware Virtual Center. Otherwise, no partition information is available when you install the agents and they are registered on the administration server with a status of `incomplete`.

Before you begin

This task has the following prerequisites:

- All guest operating systems must be active when the script runs
- On Microsoft Virtual Server systems, the Microsoft Virtual Machine Additions service must be installed and active
- VMware servers, VMware Tools must be installed on the guest operating system
- Linux The enabler requires the compat-libstdc++ library to be installed
- Red Hat The enabler requires the compatibility packs documented in *Supported platforms for agents*.

The enabler is a script that allows Common Inventory Technology to obtain information about the VMware or Microsoft Virtual Server virtualization environment. You need to run the enabler script on the target host system first, before installing the Tivoli Asset Discovery for Distributed agent, and again after every reboot or VM configuration change.

Tip: Use a scheduling service to set up the enabler to run automatically. The script does not provide its own scheduling mechanism, so you need to use an operating system function such as the cron service on UNIX computers. It is advisable to set the scheduling mechanism to run the script every day, but a different frequency might be set depending on the unique configuration of your VMs.

Note: The procedure described below installs Common Inventory Technology in the default location. To change it, for example if there is not enough space in the default directory, edit the **CITInstallPath** parameter in the agent installation response file

1. Find the files for your platform and partitioning technology in the `enabler` directory on the installation DVD, or in the .zip file for your platform if you downloaded the agent installer from the IBM Passport Advantage® Web site. Copy the files for your environment to a directory on the host virtual server system. Copy all files into the same directory

   Windows **VMware Windows (space) WMware host**

   ```
   wenvmw.exe
   cpuid.exe
   retrieve.pl
   ```

   Linux **VMware Linux (space) VMware host**

   ```
   wenvmw.sh
   cpuid
   dispatcher
   retrieve.pl
   ```

   Windows **Microsoft Virtual Server Windows host**

   ```
   wenmsvs.exe
   cpuid.exe
   ```

2. Run the enabler script using the **-v** option.
   - Windows On a VMware host, run **wenvmw.exe -v**.
   - Linux On a VMware host, run **wenvmw.sh -v**.
   - Windows On a Microsoft Virtual Server host, run **wenmsvs.exe -v**.

Log files `retr_out.txt` and `en_out.txt` are created in the same directory as the directory where you copied the files for the scirpt.

3. Check the logs to see whether the script was run successfully.

Now you can upgrade the agent on the guest system.

Disabling SELinux when installing the agent on RedHat Linux

Unlike with server installation, the permissive SELinux setting is still too restrictive for agent installation. For some kernel releases, setting SELinux to permissive will prevent the agent from being installed. To avoid this, change the setting to disabled mode.

1. Open the `/etc/selinux/config` file.
2. Set the **SELINUX** parameter to `disabled`.
3. Restart your machine.

Upgrading agents using native installers

You can upgrade agents in your infrastructure with native installers, using the existing configuration. However, you cannot use a response file to customize the parameters to upgrade the agents on multiple machines with the same operating system and basic configuration. Even if a response file is provided, it will not be used when the installer discovers an upgrade process (but not the pristine installation). If you want to change the configuration of an agent, you will need to update the parameters in the `tlmagent.ini` configuration file after the upgrade.

Upgrading agents on Windows

The installation wizard allows you to specify a number of installation parameters. Ensure that none of the parameter values contain the character #, spaces or UTF strings.

1. Log on to the computer where you want to install the agent as a user with administrative rights.
2. Copy the *INSTALLER_COMPRESSED_FILE_NAME*`.zip` file to a directory in the file system of your machine (either from a DVD or a directory where you store the files downloaded from Passport Advantage). Extract the compressed file into a directory on your disk.
3. In the directory where you have extracted the files launch the `setup.exe` file. The wizard starts and requests you to select the language version that you want to install.

   The initial panel is a welcome panel. Click **Next**.
4. A summary panel opens. Select the check box **Install the agent**. If you plan to deploy the agent on machines with the same configuration, select the check box **Save my settings in a response file** and click **Browse** to specify the folder where the file is to be saved. Click **Next** to start the installation of the agent.
5. When the upgrade is complete, click **Finish**.

Upgrading agents on UNIX systems

Before you begin

- You must have root privileges.
- If you are upgrading agents on Red Hat Linux or SUSE Linux, set the **SELINUX** variable in `/etc/selinux/config` to disabled. Restart the machine.

Turn it off with command **setenforce 0**. You can check the current security policy using **getenforce** command. If SELINUX is in permissive mode and agent still fails to install, then disabling SELINUX will help, but this solution involves rebooting the machine.

- To upgrade the agents on UNIX platforms you must have the Korn shell (ksh) installed and activated.

Machine Type is the new parameter that is added in the process of upgrading zLinux agents. Other parameter values are modified or left unchanged, as listed in the following table:

Table 36. New parameters in the upgrading of Tivoli Asset Discovery for Distributed agent to version 7.2.1

Version of the previous agent	Previous ProcessorType Parameter	New ProcessorType Parameter	New MachineType Parameter
2.3	CP	CP	z9
	IFL	IFL	z9
7.1 and 7.2	CP (if upgraded from V2.3)	CP	z9
	IFL (if upgraded from V2.3)	IFL	z9
	z9 (if pristine installation)	**IFL** (default value)	z9
	z10 (if pristine installation)	**IFL** (default value)	**z10**

Note: If you are upgrading agents on an AIX platform that is partitioned using the WPAR partitioning technology with an LPAR host, you must upgrade an agent in the LPAR before upgrading agents in the WPAR.

1. Copy the compressed installer to a directory in the file system of your machine (either from a DVD or a directory where you store the files downloaded from Passport Advantage).
2. Open a system command prompt and navigate to the directory where you store the compressed installer.
3. Uncompress the file by running the following command:

   ```
   gzip -d <INSTALLER_TARBALL_FILE_NAME>.tar.gz
   ```
4. Extract the installer files by issuing the following command:

   ```
   tar xf <INSTALLER_TARBALL_FILE_NAME>.tar
   ```

   Depending on your platform, in the directory you should have the following files:

   - AIX
     - ILMT-TAD4D-agent-aix-ppc
     - ILMT_TAD4D_72_agentInstall_response.txt
   - HP-UX
     - ILMT-TAD4D-agent-hpux_ia64
     - ILMT-TAD4D-agent-hpux_parisc
     - ILMT_TAD4D_72_agentInstall_response.txt
   - Linux
     - ILMT-TAD4D-agent-7.2-linux-x86.rpm (Linux x86) or

- ILMT-TAD4D-agent-7.2-linux-s390.rpm (Linux 390, 31 and 64–bit) or
- ILMT-TAD4D-agent-7.2-linux-ppc.rpm (Linux ppc)
- ILMT_TAD4D_72_agentInstall_response.txt

- Solaris
  - ILMT_TAD4D-agent-7.2-solaris-x86_64 (Solaris on EM64T and AMD 64) or
  - ILMT_TAD4D-agent-7.2-solaris-sparc32 (Solaris on SPARC, 32–bit) or
  - ILMT_TAD4D-agent-7.2-solaris-sparc64 (Solaris on SPARC, 64–bit) and
  - ILMT_TAD4D_72_agentInstall_response.txt

5. To upgrade the agent enter the following command:
   - AIX

     ```
     installp -acgXd <PATH_TO_INSTALLATION_PACKAGE_DIR> ILMT-TAD4D-agent
     ```

     In WPAR environments, the command is:

     ```
     installp -acgX -Or ILMT-TAD4D-agent
     ```

   - HP-UX

     ```
     swinstall -s <INSTALLER_FILE_NAME> ILMT-TAD4D-agent
     ```

   - Linux

     ```
     rpm -ihv <INSTALLER_FILE_NAME>.rpm
     ```

   - Solaris

     ```
     pkgadd -d <INSTALLER_FILE_NAME>
     ```

The agent on your machine has been upgraded. The server address has been migrated from the previous agent configuration.

To verify the upgrade, you need to run the tlmagent -v command which displays the version of the agent. You might also want to check if the agent appears in the Asset Discovery for Distributed web user interface with the active status or check the installation logs. For more information see *Agent installation trace logs* in the Troubleshooting section of the Asset Discovery for Distributed information center.

Upgrading agents on IBM i

Before you begin

Ensure you have reviewed the agent upgrade prerequisites which can be found in the Planning section of IBM Tivoli Asset Discovery for Distributed information center. There are some program temporary fixes (PTFs) in certain versions that are required for version 7.2 of Asset Discovery for Distributed. Install the required program temporary fixes before upgrading the agents on IBM i platform.

1. Copy the **SAVF** onto the target IBM i computer using any suitable method (file transfer protocol, optical drive). The file is provided in the installation package.
2. Log in to the node. The user ID should have rights that enable you to use the RSTLICPGM command.
3. Remove the agent. The configuration will be preserved and reused for the upgrading of the agent. Delete the agent by using the command: DLTLICPGM LICPGM(1IBMTLM).
4. Restore the agent by using the following command to install the agent on the target machine:

   RSTLICPGM LICPGM(1IBMTLM) DEV(*SAVF) RLS(V7R2M0) SAVF (<LIBRARY_WHERE_THE_SAVF_FILE_IS_PLACED>/<SAVF_FILE_NAME>)

The agent should start automatically, connect itself to the Asset Discovery for Distributed server and plug itself in.

To check that the agent has been correctly installed open the Installed License Programs panel on the IBM i node, and check that there is an entry for `1IBMTLM`. On the same panel, you can press F11 key to display product release. Only if 1IBMTLM product's release is V7R2M0, and it's status is *INSTALLED the agent is considered as successfully upgraded.

Upgrading V7.2 agents (installed natively) using native installers

You can upgrade V7.2 agents that were installed with the use of native installers. This upgrade process, which uses native installation files, does not change the existing configuration, so you cannot use a response file to customize the parameters to upgrade the agents on multiple machines with the same operating system and basic configuration. Even if a response file is provided, it will not be used when the installer discovers an upgrade process (but not the pristine installation). If you want to change the configuration of an agent, you will need to update the parameters in the `tlmagent.ini` configuration file after the upgrade.

Upgrading agents on Windows

Before you begin

See the "Before you begin" section of “Enabling the agent self-update” on page 171.

The installation wizard allows you to specify a number of installation parameters. Ensure that none of the parameter values contain the character #, spaces or UTF strings.

1. Log on to the computer where you want to install the agent as a user with administrative rights.
2. Copy the *INSTALLER_COMPRESSED_FILE_NAME*`.zip` file to a directory in the file system of your machine (either from a DVD or a directory where you store the files downloaded from Passport Advantage). Extract the compressed file into a directory on your disk.
3. In the directory where you have extracted the files launch the `setup.exe` file. The wizard starts and requests you to select the language version that you want to install.

   The initial panel is a welcome panel. Click **Next**.
4. A summary panel opens. Select the check box **Install the agent**. If you plan to deploy the agent on machines with the same configuration, select the check box **Save my settings in a response file** and click **Browse** to specify the folder where the file is to be saved. Click **Next** to start the installation of the agent.
5. When the upgrade is complete, click **Finish**.

Upgrading agents on UNIX systems

Before you begin

See the "Before you begin" section of “Enabling the agent self-update” on page 171.

Solaris If you are using the native installation script, you need to open the `/var/sadm/install/admin/default` configuration file, and change **instance=line** to **instance=overwrite**. Otherwise, packages will not be upgraded.

- You must have root privileges.

- If you are upgrading agents on Red Hat Linux or SUSE Linux, set the **SELINUX** variable in `/etc/selinux/config` to disabled. Restart the machine.

  Turn it off with command **setenforce 0**. You can check the current security policy using **getenforce** command. If SELINUX is in permissive mode and agent still fails to install, then disabling SELINUX will help, but this solution involves rebooting the machine.
- To upgrade the agents on UNIX platforms you must have the Korn shell (ksh) installed and activated.

Note: If you are upgrading agents on an AIX platform that is partitioned using the WPAR partitioning technology with an LPAR host, you must upgrade an agent in the LPAR before upgrading agents in the WPAR.

1. Copy the compressed installer to a directory in the file system of your machine (either from a DVD or a directory where you store the files downloaded from Passport Advantage).
2. Open a system command prompt and navigate to the directory where you store the compressed installer.
3. Uncompress the file by running the following command:

   ```
   gzip -d <INSTALLER_TARBALL_FILE_NAME>.tar.gz
   ```
4. Extract the installer files by issuing the following command:

   ```
   tar xf <INSTALLER_TARBALL_FILE_NAME>.tar
   ```

   Depending on your platform, in the directory you should have the following files:

   - AIX
     - ILMT-TAD4D-agent-aix-ppc
     - ILMT_TAD4D_7.2.1_agentInstall_response.txt
   - HP-UX
     - ILMT-TAD4D-agent-hpux_ia64
     - ILMT-TAD4D-agent-hpux_parisc
     - ILMT_TAD4D_<version>_agentInstall_response.txt
   - Linux
     - ILMT-TAD4D-agent-<version>-linux-x86.rpm (Linux x86) or
     - ILMT-TAD4D-agent-<version>-linux-s390.rpm (Linux 390, 31 and 64–bit) or
     - ILMT-TAD4D-agent-<version>-linux-ppc.rpm (Linux ppc)
     - ILMT_TAD4D_<version>_agentInstall_response.txt
   - Solaris
     - ILMT_TAD4D-agent-<version>-solaris-x86_64 (Solaris on EM64T and AMD 64) or
     - ILMT_TAD4D-agent-<version>-solaris-sparc32 (Solaris on SPARC, 32–bit) or
     - ILMT_TAD4D-agent-<version>-solaris-sparc64 (Solaris on SPARC, 64–bit) and
     - ILMT_TAD4D_<version>_agentInstall_response.txt
5. To upgrade the agent enter the following command:

   - AIX

     ```
     installp -acFxd <PATH_TO_INSTALLATION_PACKAGE_DIR> ILMT-TAD4D-agent
     ```

In WPAR environments, the command is:

```
installp -acFx -Or ILMT-TAD4D-agent
```

- HP-UX

```
swinstall -x reinstall=true -s <INSTALLER_FILE_NAME> ILMT-TAD4D-agent
```

- Linux

```
rpm -Uhv <INSTALLER_FILE_NAME>.rpm
```

- Solaris

```
pkgadd -d <INSTALLER_FILE_NAME>
```

The agent on your machine has been upgraded. The server address has been migrated from the previous agent configuration.

To verify the upgrade, you need to run the tlmagent -v command which displays the version of the agent. You might also want to check if the agent appears in the Asset Discovery for Distributed web user interface with the active status or check the installation logs. For more information see *Agent installation trace logs* in the Troubleshooting section of the Asset Discovery for Distributed information center.

Using IBM Tivoli Configuration Manager to install the agents in bulk

For environments where Configuration Manager is installed, you can use its software distribution function to deploy the agents to endpoints as software packages.

Before you begin

Ensure that you have the appropriate version of Tivoli Configuration Manager and Tivoli Management Framework installed in your environment:

iSeries and pSeries platforms

- Management Framework 4.1 with fixes 4.1-TMF-0015 for Linux-PPC (server) and 4.1-INVGW-0005 for Linux-PPC (gateway) installed
- Configuration Manager 4.2 with fixes 4.2-SWD-0014 (server) and 4.2-SWD-0015 (gateway) installed

zSeries platforms

- Management Framework 4.1.1
- Configuration Manager 4.2.1

Other platforms

- Management Framework 4.1
- Configuration Manager 4.2.

Depending on the platform, you also need 20 – 30 MB of disk space for the software package block that is to be distributed.

The Tivoli Asset Discovery for Distributed Software Package DVD contains an agent installation SPB for each supported platform:

- AIX aix_superspb.spb
- HP-UX hpux_ia64_superspb.spb
- HP-UX hpux_parisc_superspb.spb

- i5/OS os400agent_superspb.spb
- Linux linux_superspb.spb
- Linux linux390_superspb.spb
- Linux linuxppc_superspb.spb
- Solaris sun32_superspb.spb
- Solaris sun64_superspb.spb
- Solaris sun_x86_superspb.spb
- Windows win32_superspb.spb

1. Copy the software package block for your platform from the DVD to a directory on the TMR server or a managed node.
2. Ensure that the Tivoli Environment is configured.
3. Create a profile manager for each SPB that you want to distribute.
4. Import the SPBs.
5. Perform distributions using the force option to install the appropriate platform-specific agent SPB on each target computer.

   You must provide values for the configuration parameters during the distribution. See the related links section for a complete definition of the software package block and the possible values that can be assigned to each parameter.

Upgrading agents with Windows logon scripts

As an alternative to using the interactive installation wizard, you can install Asset Discovery for Distributed agents on Windows targets by using the operating system facility that runs a script when users log on to the Windows domain.

The script checks to see whether there is an agent on the computer from which the user has logged on, and if there is, whether it is the same version. If the script finds no agent or a back-level agent, it installs the agent.

1. Log in to the Windows domain controller.
2. Find or create the NETLOGON shared directory. You should not grant write permissions to the directory to all users in the domain. The contents of the shared directory should be as follows:
   - getdt.exe
   - gethost.exe
   - getos.bat
   - printmsg.exe
   - profiles
   - setAgentReturnCode.bat
   - sethostname.bat
   - setup.exe
   - tlm.bat
   - tlminstall.bat
   - profiles/default.conf

   If the user account that you are using for the installation has Domain Administrator rights, you can also set up a shared directory for logs so that the actions of the scripts are logged on the domain server.

3. Specify the script `\tlm.bat` in the user profile of the Domain User Manager. Set the script to run automatically when logging in to the domain account.
4. Set the following values for the environment variables in the `\tlm.bat` file in the NETLOGON directory:

   ```
   set DOMAINSERVER=DOMAIN_SERVER
   set NETLOGON_SHARE=NETLOGON_SHARE
   set LOG_SHARE=LOG_SHARE
   ```

   where:

   DOMAIN_SERVER
   The host name of the Windows domain controller.

   NETLOGON_SHARE
   The share name of the NETLOGON share.

   LOG_SHARE
   The share name of the LOG share where the logs are to be stored. If you do not want to log the running of the script, change the variable to be blank.
5. Set the agent installation parameters in the `profiles\default.conf` configuration file. You must configure parameter values for at least the scan group and server. You can leave the other parameters as defaults.
   - If you are assigning all computers in the domain to the same organization, scan group, and server, you can use this file to deploy all the agents.
   - If you are assigning some computers a different configuration, you can create copies of the default file, named `profiles\hostname.conf` (where *hostname* is the host name of the computer to which the configuration is to be applied) and define different configurations in these files.

   For parameter descriptions, see *Agent installation response file and Windows logon script configuration file*.
6. Log in to the system on which the agent is to be installed. Use the domain user account.

   Note: Ensure that you belong to the local Administrators group on the computer where the agent is installed.
7. If the IBM Global Security Kit (GSKit) is already in use, reboot the computer to complete the installation.

Performing a refresh installation of agents

Performing a refresh installation of Tivoli Asset Discovery for Distributed agents allows you to refresh them without changing their configuration parameters. You can do this by reinstalling them manually.

Before you begin

Solaris If you are using the native installation script, you need to open the `/var/sadm/install/admin/default` configuration file, and change **instance=line** to **instance=overwrite**. Otherwise, packages will not be refreshed.

1. Copy the compressed installer to a directory in the file system of your machine (either from a DVD or a directory where you store the files downloaded from Passport Advantage).
2. Open a system command prompt and navigate to the directory where you store the compressed installer.
3. Uncompress the file by running the following command:

```
gzip -d <INSTALLER_TARBALL_FILE_NAME>.tar.gz
```

4. Extract the installer files by issuing the following command:

   ```
   tar xf <INSTALLER_TARBALL_FILE_NAME>.tar
   ```

   Depending on your platform, in the directory you should have the following files:

   - AIX
     - ILMT-TAD4D-agent-aix-ppc
     - ILMT_TAD4D_7.2_agentInstall_response.txt
   - HP-UX
     - ILMT-TAD4D-agent-hpux_ia64
     - ILMT-TAD4D-agent-hpux_parisc
     - ILMT_TAD4D_7.2_agentInstall_response.txt
   - Linux
     - ILMT-TAD4D-agent-7.2-linux-x86.rpm (Linux x86) or
     - ILMT-TAD4D-agent-7.2-linux-s390.rpm (Linux 390, 31 and 64–bit) or
     - ILMT-TAD4D-agent-7.2-linux-ppc.rpm (Linux ppc)
     - ILMT_TAD4D_7.2_agentInstall_response.txt
   - Solaris
     - ILMT_TAD4D-agent-7.2-solaris-x86_64 (Solaris on EM64T and AMD 64) or
     - ILMT_TAD4D-agent-7.2-solaris-sparc32 (Solaris on SPARC, 32–bit) or
     - ILMT_TAD4D-agent-7.2-solaris-sparc64 (Solaris on SPARC, 64–bit) and
     - ILMT_TAD4D_7.2_agentInstall_response.txt

5. To perform a refresh installation of an agent enter the following command:

   - AIX

     ```
     installp -acgXd PATH_TO_INSTALLATION_PACKAGE_DIR ILMT-TAD4D-agent
     ```

     In WPAR environments, the command is:

     ```
     installp -acgX -Or ILMT-TAD4D-agent
     ```

     If the agent was installed using a native installer the command is:

     ```
     installp -acFxd PATH_TO_INSTALLATION_PACKAGE_DIR ILMT-TAD4D-agent
     ```

     In WPAR environments, the command is:

     ```
     installp -acFx -Or ILMT-TAD4D-agent
     ```

   - HP-UX

     ```
     swinstall -s INSTALLER_FILE_NAME ILMT-TAD4D-agent
     ```

     If the agent was installed using a native installer the command is:

     ```
     swinstall -x reinstall=true -s INSTALLER_FILE_NAME ILMT-TAD4D-agent
     ```

   - Linux

     ```
     rpm -ihv INSTALLER_FILE_NAME.rpm
     ```

     If the agent was installed using a native installer the command is:

     ```
     rpm -ihv --force INSTALLER_FILE_NAME.rpm
     ```

   - Solaris

     ```
     pkgadd -d INSTALLER_FILE_NAME
     ```

If the agent was installed using a native installer the command is the same.

The agent files on your computer have been refreshed.

Troubleshooting and support

This section explains how to find logs, messages, and trace files that you might need to troubleshoot issues that could arise with the IBM Tivoli Asset Discovery for Distributed server, agents, and other components that are part of the application.

Accessing problem determination information

This section explains how to find a wide range of IBM Tivoli Asset Discovery for Distributed information including messages, logs, and trace information for the server and the agent.

Message files

The infrastructure elements of Asset Discovery for Distributed generate messages that are classified as errors, warnings, and information. All error messages and many warning messages recommend an action to resolve the situation that the message identifies.

Message file locations

Message files for all infrastructure elements are named `Msg-<number>.log`, where <*number*> identifies the iteration of the file (the most current file is with the lowest number). They are created in the following directories on the computers where the infrastructure element is installed:

Administration server
`<TIVOLI_COMMON_DIR>/COD/logs/admin/message/` and `<TIVOLI_COMMON_DIR>/COD/logs/admin/message/cli/`

Agent `<TIVOLI_COMMON_DIR>/COD/logs/agent/message/`

WebSphere Application Server agent
`<TIVOLI_COMMON_DIR>/COD/logs/was_agent/message/`

Message handler
`<TIVOLI_COMMON_DIR>/COD/logs/msghandler/message/`

Installation/uninstallation process
`<TIVOLI_COMMON_DIR>/COD/logs/install/message/` (for both the server and agent)

Message structure

The infrastructure elements generate messages that are classified as errors, warnings, and information. All error messages and many warning messages recommend an action to resolve the situation that the message identifies. To view detailed information about the message elements, see: Message elements.

Accessing messages

All error and warning messages are written to the message logs. If a problem is generated by an operation performed on one of the GUIs, the message is displayed on the screen. Other messages are logged silently.

Messages for the server, agent, WebSphere agent, and the command line are logged in XML format in the language currently in use. To read these logs, use the viewer command.

The problem determination tool command (pdtool) provides a more specialized analysis of the server and message logs. It is designed to identify occurrences of a defined set of problems that can be resolved by changing configuration values or environment settings, for example, a misconfiguration of a server.

On the agent infrastructure element, most messages are logged silently. When agent messages are displayed, for example, when the agent command line is used, only the message text is displayed.

Configuring event notifications

You can configure the server to generate email notifications of significant licensing and system administration events. The notifications are then sent to recipients that you select in the Web interface.

You can configure event notifications using the `system.properties` file. For details of the types of notification that can be generated on the server, see the "Troubleshooting and support" section of the information center.

1. Open the`system.properties` file.
   - If the server was installed on the bundled version of WebSphere Application Server, the file is located at `<INSTALL_DIR>/eWAS/systemApps/isclite.ear/tad4d_admin.war/WEB-INF/conf`.
   - For the stand-alone version of WebSphere Application Server, the file is located at `<INSTALL_DIR>WebSphere/AppServer/systemApps/isclite.ear/tad4d_admin.war/WEB-INF/conf`.
2. Specify the following parameters:

   smtpServer
   The IP address of your SMTP server.

   mailSender
   The e-mail address from which the notifications will be sent.
3. Restart the server.
4. Log into the Integrated Solutions Console as an administrator.
5. In the navigator pane, select **Tivoli Asset Discovery for Distributed** → **Administration** → **Manage Notifications**.
6. Select **Add Subscriber** from the dropdown list, and click **Go**.
7. In the Add Notification Subscriber page, specify the recipient of notification e-mails, and the events to which they are assigned.
8. Click **OK** to save and close, or **Save and Add Another** to add another recipient.

Event logs files

Asset Discovery for Distributed includes a component that logs significant events that occur on the administration server, such as when the server starts or stops.

Event log location and size

The event log for the server is located at the following path:
`Administration server: <TIVOLI_COMMON_DIR>\COD\logs\admin\event`

The number of event log files that are maintained and the maximum size of each file are configurable and are defined in the `log.properties` file for the server. The event logging component always writes to the file `event-0.log`. When this file reaches its maximum size, it is renamed `event-1.log` and a new `event-0.log` is started. If `event-1.log` already exists, it is renamed `event-2.log` and so on, until the maximum number of files is reached. The oldest log is always the file with the highest number. The most current log is always `event-0.log`.

Server information

If problems occur with the installation or operation of the administration server, you can view trace logs and message logs for troubleshooting.

Server installation and upgrade trace logs:

The traces for the installation or upgrade of servers and related databases provide a detailed, timestamped record of the actions taken during installation and any exceptions that occurred.

The trace files produced by the installer are stored in the following directory: `<TIVOLI_COMMON_DIR>\COD\logs\install\trace`.

The following trace logs are created:

`trace_servers.log`
: This is the main installation log written by the wizard that installs the server and related databases (the log is also created during the upgrade process). It traces the installation process from beginning to end including the checks for prerequisites and for the existence of a previous or current version of Asset Discovery for Distributed. It is written in Log XML format and can be viewed using the standard Tivoli XML Log Viewer or a text editor.

  When servers are installed, the log includes records of all validations, file creations, or updates. In the case of the automatic installation of prerequisites, the log records the entry and exit for this phase of installation, while the details of the installation are recorded in the installation logs of the prerequisite products. Similarly, when a database is installed, this log records the entry and exit into the phase of database creation and population, while the details are recorded in the `trace_db_servers.log` file.

`Server.log`
: This log can be used by advanced users during problem investigation. It is located in the following directory:

  - `/tmp/tad4d` (on UNIX)
  - `%TEMP%\tad4d` (on Windows)

`trace_db_servers.log`
: This log is written by the installation wizard when the option to install a database has been selected. It traces the installation phase during which the database is created, configured, and (in the case of the administration

server database) populated with the information relating to products that can be monitored by the administration server. This log is a text file and can be viewed in any text editor.

ewas.log
This log contains the output of jacl scripts run by the installer.

DB2install.log
This is the log written by the wizard that installs the DB2 database. It is located in the following directory:

- <*TIVOLI_COMMON_DIR*>/COD/logs/install/trace/DB2install.log (on UNIX)
- <*TIVOLI_COMMON_DIR*>\COD\logs\install\trace\DB2install.log (on Windows)

Note: The trace_servers.log file is created as soon as the installation wizard starts. This means that they exist before the Tivoli common directory structure is created. If the install fails before it has created the Tivoli common directory structure, the log file is saved in the following directory: Windows %TEMP% or UNIX /tmp. Depending on your system settings, the %TEMP% directory may be hidden. To locate the directory, issue the command echo %TEMP% to find out the directory name. You can then specifically open the log file.

Server installation message logs:

The installer generates messages, some of which are displayed on the wizard panels either when a situation occurs or in a summary at the end of the wizard.

All messages are logged in the msg_servers.log file, which is stored in the following directory: <*TIVOLI_COMMON_DIR*>\COD\logs\install\message.

Note: Installation message logs are written in Log XML format and can be viewed using the standard Tivoli XML Log Viewer or any text editor.

Server trace logs:

The trace component that is used on the administration server and command-line interface is able to collect a wide range of information. A minimum level of tracing is enabled by default and cannot be disabled to ensure that some trace information is always available when a problem occurs. Thus, you will only need to set a higher trace level and try to reproduce the problem if the default logged information is insufficient.

Trace levels

The following table shows how to modify the three levels of tracing:

Table 37. Trace levels for the server

Trace level	Trace type	Description
DEBUG_MIN (default)	ERROR	Records the occurrence of unrecoverable interruptions of the workflow.
	LOG	Records significant events in the normal operation of the system, which might be of use in tracking the root of any problem that occurs.
	START/STOP	Records time-stamped entries for the start and end of threads.
	ENTRY/EXIT	Records the entry and exit points of key methods.
DEBUG_MID	TRACE	Tracks significant events.
	ASSERT	Tracks situations of high risk, for example, those that might lead to data corruption.
DEBUG_MAX	DEBUG	Provides a detailed record of the sequence of actions generated by the program code.
	DATA	Provides a detailed record of all data operations.

Trace file location and type

The administration server trace log is located at the following path:

- **Administration server:**<*TIVOLI_COMMON_DIR*>\COD\logs\admin\trace
- **Command line:** <*TIVOLI_COMMON_DIR*>\COD\logs\admin\trace\cli

The following trace types write entries to the trace log:

- DATA
- DEBUG
- ERROR
- ENTRY
- EXIT
- LOG
- START
- STOP
- TRACE

Trace file contents

Each trace message contains the following elements:

Table 38. Trace file contents

Element	Example content
Trace level	MIN
Date and time of logging	2008-05-31 00:36:43.890+02:00
Server hostname	nc044103
Product ID	COD

Table 38. Trace file contents (continued)

Element	Example content
Component	Install
Trace message	Common Directory creation was successful.
Trace source	Source FileName=⌂com.ibm.pl.krak.slm.install.wizardx.actions. TivoliCommonDirAction⌂ Method=""
Thread	Thread-2

Below is a sample trace tag:

```
<Trace Level="MIN">
<Time Millis="1212187003890">2008-05-31 00:36:43.890+02:00</Time>
<Server Format="IP">nc044103</Server>
<ProductId>COD</ProductId>
<Component>Install</Component>
<ProductInstance></ProductInstance>
<LogText><![CDATA[Common Directory creation was successful.]]></LogText>
<Source FileName="com.ibm.pl.krak.slm.install.wizardx.actions.
TivoliCommonDirAction" Method=""/>
<Thread>Thread-2</Thread>
<Principal></Principal>
</Trace>
```

Agent information

Agents create installation logs and deployment trace logs that you can use for troubleshooting. You also can analyze return codes that agents generate if they encounter problems during installation or during normal operation.

Agent installation trace logs:

Several log file are created during agent installation. All are text files and can be opened in any text editor.

All agent install logs are stored in the following directory: <*TIVOLI_COMMON_DIR*>\COD\logs\install\trace, except for the GSK Install logs which are in the var\itlm\swdis_tmp\logs directory for UNIX and \itlm\swdis_tmp\logs for Windows.

The agent installer produces the following trace log files:

traceInstallagent.log
The main log for the agent install process.

ILMT-TAD4D-agent-*timestamp*.trc
The installation log for native packages installation process.

GSKinstall.log
This log traces the installation or upgrade of GSKit. The installation process for GSKit is invoked by the installagent program. In some circumstances, the installation of GSKit will require a reboot of the computer and the agent cannot be used until this has been done. This file includes an overall result code and return codes that indicate the requirement for a reboot and the presence of files that could not be upgraded because they were locked. In the case of locked files, the changes to be made will be made automatically on reboot.

traceGSKInstaller.log
This log traces the GSKit Installer.

traceDeployagent.log
This log traces the installation or upgrade of the agent SPB.

traceAgentController.log
This log traces the stopping and starting of the agent.

traceTarballInstaller.log
This log traces installation of the NLS language codeset.

Note: The `traceInstallagent.log` file produced during installation of an agent on an i5/OS node does not include detailed information about the installation process. It includes mainly information about the actions of the wizard that deploys the agent package and launches a native program to add the agent. It also includes a return code indicating the success or failure of the native installation. To see detailed logging from the native program, you must view its log while the program is an active job.

Agent deployment trace logs:

Several log files are created during agent deployment. All are text files and can be opened in any text editor.

Tracing of the deployment phase depends on the method of deployment used:

- **Configuration manager deployment**: The Configuration Manager can be used to distribute a set of agents to target computers. When the agent is deployed using this method, trace files containing Configuration Manager information about the deployment are created in the following directories:
  - `<TARGET_DIR>\agent\logs`
  - `<TEMP_DIR>\agent\logs`

  `Target_DIR` is the name of the directory on the target computer to which the software package was sent. `Temp_DIR` is the system temporary directory `tmp` (UNIX) or `temp` (Windows)
- **Deployment on i5/OS**: The deployment process for i5/OS nodes differs from the processes available for other platforms. It does not consist of a deployment phase followed by the running of the `installagent` program. The agent is installed by launching a wizard on a Windows node. The wizard accepts the deployment parameters and launches native programs on the i5/OS node to add the agent as a program. The wizard traces its own activity, which includes the process of delivering the package to the i5/OS node, in the file `trace_agent.log` which is stored in the directory `/QIBM/UserData/tivoli/common/install/trace`.

  This log will help you to identify any problems with an i5/OS agent deployment that are external to the native program. The log is written in text format and can be opened in any text editor. If a problem occurs when installing the agent on an i5/OS node using the ISMP wizard run on a Windows computer, do not exit from the wizard before attempting to discover the cause of the problem. Trace information about the installation is recorded in the `QUSRWRK` system job log, which is cancelled when the wizard finishes either successfully or unsuccessfully.

Agent installation return codes:

If the agent installation fails, make note of the agent installation return code. The return codes are written to the `slmrc` file, except for code 102 which is written to the `slmr` file.

The table below lists return codes logged during the process of agent installation.

Table 39. Agent installation return codes

Return code	Possible cause	Solution
0	Installation successful.	
30	The agent has been successfully installed, but the computer must be rebooted before the agent can start.	Reboot the computer. The agent will start automatically when the computer restarts.
102	The agent can be installed.	Install the agent. This return code is logged in the file slmr when all checks have been completed and the agent is ready to install. When the agent is installed, this code is deleted. Therefore, the presence of this code indicates that the agent installation was interrupted for a reason not connected with errors or problems discovered during the checks.
-1	An unexpected error occurred during initial phase of agent deployment.	Retry the installation and if the problem persists, contact IBM Software Support.
-2	The Windows environment variable *%WINDIR%* does not exist or the folder containing the agent installation files could not be created.	Verify that the variable exists by checking **My Computer → Properties → Advanced → Environment Variables**. Also verify that you have the necessary security permissions for the creation of the folder containing the agent installation files and check that there is sufficient space on the disk.
-3	The agent configuration file `tlmagent.ini` could not be written to the temporary installation directory.	Check the disk and file systems where the agent configuration files should be installed and verify the following: • You have write access to the folder • Check for locked files and unlock them • Verify if there is sufficient space on the disk.
-4	Failure to copy agent file from temporary installation directory to destination directory.	Verify that you have write access to the folder containing the agent installation files. Also check for locked files and unlock them and verify that there is sufficient space on the disk.
-5	An error occurred while attempting to write reboot file to disk during the installation of the IBM Global Security Toolkit (GSKit).	Verify that you have write access to the folder containing the agent installation files. Also check for locked files and unlock them and verify that there is sufficient space on the disk.
- 8	The agent failed to start for one of the following reasons: • Wrong parameters in `tlmagent.ini` file • Other internal error.	Reinstall the agent specifying the correct parameters.

Table 39. Agent installation return codes (continued)

Return code	Possible cause	Solution
-13	The agent uninstall script could not be installed.	Check the disk and file systems where the agent configuration files should be installed and verify the following: • You have write access to the folder. • Check for locked files and unlock them • Check that there is sufficient space on the disk.
-14	You do not have sufficient privileges to install the agent.	Log on to the computer as a user with administrative rights (root for UNIX).
-16	The tables and files for national language support could not be copied to the temporary directory.	Check the disk and file systems where the agent configuration files should be installed and verify the following: • You have write access to the folder. • Check for locked files and unlock them • Check that there is sufficient space on the disk.
-17	Failure to write the agent signature file to the agent installation folder.	Check the disk and file systems where the agent configuration files should be installed and verify the following: • You have write access to the folder. • Check for locked files and unlock them • Check that there is sufficient space on the disk.
-19	The target node currently has an agent installed and the organization name for the current agent does not match the organization name of the server specified for the new agent.	If the target node is to be transferred to a different organization, you must uninstall the current agent before deploying the new agent. Reinstall the agent specifying the correct organization name.
-20	An error occurred on a Linux 390 computer while writing the `tlmsubcapacity.cfg` file.	Check the disk and file systems where the agent configuration files should be installed and verify the following: • You have write access to the folder. • Check for locked files and unlock them • Check that there is sufficient space on the disk.
-21	An internal error occurred while initializing the agent configuration.	The `tlmagent.ini` file already exists and is locked or another installation is currently running locking the configuration file. Contact IBM Software Support if neither of these solutions solves the problem.
-22	GSKit could not be installed. Therefore, the installation of the agent could not proceed.	Check the prerequisites for the installation of the agent and that you have the appropriate permissions to perform the installation.

Table 39. Agent installation return codes (continued)

Return code	Possible cause	Solution
-23	It is not possible to copy the GSKit package to the system temporary folder.	• Ensure the path to the system temporary folder is not too long and retry the installation. • Check that you have write access to the folder. • Check for locked files and unlock them. • Check that there is sufficient space on the disk.
-29	The agent has not been correctly registered as a service on the target node.	• On Windows platforms, the Windows services panel was open during the installation. Close the panel and retry the installation. • On UNIX platforms, retry the installation.
-33	Failure to create a backup of existing agent files and directories during agent deployment.	Check that there is sufficient space on the disk.
-39	Installation of agent failed in a partitioned environment because prerequisite tools are not installed or are inactive.	• Install or start the Microsoft® Virtual Machine Additions service. • Install VMware tools. • Install VM tools on HP Itanium® guests.
-101	An unexpected error occurred during initial phase of agent deployment.	Retry the installation and if the problem persists, contact IBM Software Support.
-102	Error parsing agent installation parameters.	The installer does not allow non-Latin characters when specifying paths (i.e. agent installation path, Common Inventory Technology installation path, agent temporary folder etc.) and scan group name. Ensure that the path and scan group names contain no national characters, then retry the installation. If you need to add the agent to a scan group that has non-Latin characters in its name, add it to a different group at installation time, then reassign it to the target scan group after the installation finishes.
-104	An unexpected error occurred during initial phase of agent deployment.	Retry the installation and if the problem persists, contact IBM Software Support.
-201	Before installing the new agent, an attempt to stop a previously deployed agent failed.	• Try to stop the previously deployed agent manually and retry the installation. • If you do not need to maintain the previously deployed agent configuration, then uninstall the agent and retry the installation.

Table 39. Agent installation return codes (continued)

Return code	Possible cause	Solution
-202	An unexpected error occurred while attempting to start or stop the agent.	Retry the installation and if the problem persists, contact IBM Software Support.
-203	An unexpected error occurred while attempting to start or stop the agent.	Retry the installation and if the problem persists, contact IBM Software Support.
-205	The agent could not be started because you entered incorrect capacity values.	If you are installing agent on zLinux, launch the installation again and provide proper capacity values. For more information on these parameters, refer to section *Installing the agent on Linux for zSeries* of *Planning, installation and configuration* book. On other platforms, this indicated an internal error and you need to contact IBM support to solve this issue.
-303	An unexpected error occurred while attempting to install GSKit.	Retry the installation and if the problem persists, contact IBM Software Support.
-304	An unexpected error occurred while attempting to install GSKit.	Retry the installation and if the problem persists, contact IBM Software Support.
-401	An unexpected error occurred while attempting to install the SPBs related to national language support or the software distribution disconnected command line.	Retry the installation and if the problem persists, contact IBM Software Support.
-402	Failed to extract files related to national language support or the software distribution disconnected command line.	• Check that you have write access to the agent installation folder. • Check for locked files and unlock them. • Check that there is sufficient space on the disk.
-403	Failure to create a backup of existing national language support files or software distribution disconnected command line files.	Check that there is sufficient space on the disk.
-500	Failed to extract files related to the software distribution disconnected command line.	• Check that you have write access to the system temporary folder. • Check for locked files and unlock them. • Check that there is sufficient space on the disk. • The packet might be corrupt. You can try to deploy the agent again. • If this works, the packet is corrupt only on the original source server. If it does not work, contact IBM Software Support.

Table 39. Agent installation return codes (continued)

Return code	Possible cause	Solution
-502	Failed to install the software distribution disconnected command line SPB: TIVOLI_ITLM_AGT_SWDCLI_INST_<*platform*>.	• Check that you have write access to the system temporary folder. • Check for locked files and unlock them. • Check that there is sufficient space on the disk. • The packet might be corrupt. You can try to deploy the agent again. • If this works, the packet is corrupt only on the original source server. If it does not work, contact IBM Software Support.
-503	Failed to install the software distribution disconnected command line SPB: TIVOLI_ITLM_AGT_GSKIT_<*platform*>.	• Check that you have write access to the system temporary folder. • Check for locked files and unlock them. • Check that there is sufficient space on the disk. • The packet might be corrupt. You can try to deploy the agent again. • If this works, the packet is corrupt only on the original source server. If it does not work, contact IBM Software Support.
-504	Failed to install the Common Inventory Technology infrastructure element `SPB, CIT_Preinstall.spb`.	• You might not have enough space. Check that there is sufficient space in the component directory to unpack the files. • The packet might be corrupt. You can try to deploy the agent again. If it does not work, contact IBM Software Support.
-505	Failed to install Common Inventory Technology infrastructure element `SPB, CIT_<platform>.spb`.	You might not have enough space. Check that there is sufficient space in the component directory to unpack the files. The packet might be corrupt. You can try to deploy the agent again. If it does not work, contact IBM Software Support.

Table 39. Agent installation return codes (continued)

Return code	Possible cause	Solution
-507	Failed to install the software distribution disconnected command line SPB: TIVOLI_ITLM_AGT_AGENT_<*platform*>.	• Check that you have write access to the system temporary folder. • Check for locked files and unlock them. • Check that there is sufficient space on the disk. • The packet might be corrupt. You can try to deploy the agent again. • If this works, the packet is corrupt only on the original source server. If it does not work, contact IBM Software Support

Agent operation error codes:

This section provides a list of error codes for the agent. For some agent problems, the symptom is detected at the server. For others, the system administrator might receive a communication from the application user on whose system the agent is running, sometimes by way of the license administrator. Some of the solutions require the system administrator to ask the application user to take some action, such as enter a specific command.

The table below lists return codes logged during the agent operation.

Table 40. Agent error codes from CLI trace logs

Error code	Description
1	General CLI error. Most probably wrong command or its syntax.
2	The agent must be running to execute the command.
4	Problem in communication with the agent daemon. Try restarting the agent.
6	Warning during stopping the agent - agent is already stopped (not running).
7	Problem in communication with the agent daemon. Try restarting the agent.
9	Problem in communication with the agent daemon. Try restarting the agent.
10	Error when starting the agent. Check if service is registered.
11	Error when stopping the agent. Check if service is registered.
12	Warning during starting the agent - the agent is already started.
13	The agent service is not installed.
14	Error deleting the agent service.
15	Warning when trying to register the agent service - already registered.
16	Error during registering the agent service.
18	Error when scheduling the command. Restart the agent and try again.
22	Error during reloading of the agent configuration file. Repair the `tlmagent.ini` file and try again.
23	Error loading `tlmlog.properties` file. Repair the file and try again.
24	The command is not supported on this platform.

Table 40. Agent error codes from CLI trace logs (continued)

Error code	Description
25	Error - unknown command.
26	Warning - minor error occurred when loading the configuration file. Some properties will have default values.
28	Error initializing Common Inventory Technology component. Check if the component is properly installed.
29	Error during importing the certificate. Check if the certificate is correct.
30	Error during importing the certificate - agent ID in the certificate does not match the real agent ID.
31	Error during importing the certificate - organization in the certificate does not match the organization in the `tlmagent.ini` file.
32	Error during importing the certificate - wrong password.
33	Error during importing the certificate - system time is not in the certificate validity period.
34	Error during importing the certificate - file does not exist.
35	Error during importing the certificate - failed to extract the certificate information from file.
37	Warning during importing certificate - the agent has already more recent certificate.
38	Server time is not synchronized with agent time.
39	Agent catalog version is not aligned with server catalog. New catalog must be downloaded.
40	Error during import of catalog. Given file does not exist.
41	Error importing catalog.
42	Error exporting catalog.
43	Error exporting catalog - the file was not provided with full path.
47	Error during executing software scan. Probably Common Inventory Technology failed - examine the component traces.
48	Error during executing hardware scan. Probably Common Inventory Technology failed - examine the component traces.
49	Error during uploading scan data to server - plugin failed.
50	Error uploading scan data to the server. Check connection parameters and server condition. Then try again.
51	Warning during execution of software scan - scan is already in progress or catalog is not downloaded yet.
52	Error setting agent parameter - provided key is not valid.
53	Warning when setting agent parameter - the key is not re-loadable and will not be reloaded. Restart agent to reload the key.
54	Error during setting configuration property - key or value are not proper.
55	Error - certificate has expired.
56	Error - failed to initialize the service on Windows.
58	Error during agent start - some GSKit prerequisites are missing.
59	Error - sslreload option is not valid when plain communication is used.
60	Error capacity values are inconsistent.

Table 40. Agent error codes from CLI trace logs (continued)

Error code	Description
61	Mobility is pending (not an error).
62	Data upload is pending (not an error).
63	Hardware scan is pending (not an error).

The table below lists inventory error codes logged during the agent operation.

Table 41. Agent inventory error codes

Error code	Possible Cause	Solution
-1	An internal error occurred.	Contact IBM Software Support.
-2	Memory allocation error.	Ensure that you have enough free memory.
-3	An internal agent error occurred.	Contact IBM Software Support.
-4	Agent cache error occurred.	Delete the `inventory.dat` file and try again.
-10	An internal occurred in the scan logic.	Contact IBM Software Support.
10	The scan has been aborted by the user.	Try the scan again.
30	An internal occurred in the scan logic.	If necessary, try the scan again later.
31	The scan has been aborted by the user.	Delete the file `inventory.dat` and try again.

Disabling rollback

When the installation of an agent is not successful, any changes that have been made to the target computer by the failed installation process are rolled back, leaving the environment ready for a fresh installation. On Windows and UNIX platforms you can disable this feature so that the failed installation is not removed from the target computer.

Disabling rollback allows you and IBM support to investigate the state of the installation at the point when it failed. This is useful if you are unable to identify the source of the problem from either the return code or the FFDC.

Note: On i5/OS platforms rollback is disabled by default. Note also that if you use native installers, on AIX and Windows, the system registry is cleaned up no matter what the disableRollBack value is.

1. On Windows platforms, type the following command into the system command prompt: `set disableRollBack=yes`.
2. On UNIX platforms, add the following line to the agent installation response file at agent installation: `disableRollBack=yes`.

WebSphere agent trace logs

As with the Asset Discovery for Distributed agents, the trace component that is used on agents for the WebSphere Application Server is able to collect a wide range of information. A maximum level of tracing is enabled by default to ensure that sufficient information to reproduce the problem is always logged.

Trace levels

You can set tracing to one of three levels (MIN, MID, and MAX). The following table shows the types of information that are logged at the default MAX level, and types of information that are added as the trace level is decreased to MID or MIN:

Table 42. Trace levels for the WebSphere agent

Trace level	Description
MIN	• The occurrence of unrecoverable interruptions of the workflow. • Significant events in the normal operation of the system, which might be of use in tracking the root of any problem that occurs. • Time-stamped entries for the start and end of threads. • The entry and exit points of key methods.
MID	• Significant events. • Situations of high risk, for example, those that might lead to data corruption.
MAX (default)	• Detailed records of the sequence of actions generated by the program code. • Detailed records of data operations.

Trace file location and type

The agent trace logger always writes to the file `trace.log`. When this file reaches its maximum size, it is renamed `trace1.log` and a new `trace.log` is started. If `trace1.log` already exists, it is renamed `trace2.log` and so on, until the maximum number of files is reached. The oldest log is always the file with the highest number.

The trace file is located at the following path: `<TIVOLI_COMMON_DIR>/COD/logs/was_agent/trace`.

Trace file contents

Each trace message contains the following elements:

Table 43. Trace file contents

Element	Example content
Trace level at time of logging	MIN
Date and time of entry	2005-10-19 09:18:15.000+02:00
Trace message	Adding new entry to server list name: IBM_TLM_Administration_Server soapPort: 8881 rmiPort: 2810 hostname: lab238057
Source	FileName=⌂com.ibm.it.rome.wasagent.Scanners⌂ Method=⌂scanServers⌂
Thread	Thread-4

Common Inventory Technology information

If problems occur with the Common Inventory Technology component of the product, you can use the return codes for troubleshooting.

Installation and uninstallation return codes:

Some return codes can be logged during the installation and uninstallation of Common Inventory Technology. In case of errors, use the codes to determine the root of the problem.

Table 44. Common Inventory Technology installation and uninstallation return codes

Return code	Encountered during	Description
0	Installation	Installation successful.
11	Uninstallation	Common Inventory Technology cannot be removed at this time because other exploiters are using it. Common Inventory Technology is uninstalled only when the last exploiter uninstalls it. This return code does not indicate an error. The product is working as designed.
12	Installation and uninstallation	You have not specified the exploiter label. To specify the exploiter label: • At installation time: Use the **-D** option with the `wdinstsp` command • At uninstallation time: Specify the *CIT_ExploiterID=exploiterID* environment variable in the shell used to run the `wdrmvsp` command
13	Uninstallation	The exploiter you specified is not listed in the `cit.ini` file. Check the exploiter ID then try the command again.
14	Installation	The user performing the installation does not have write access to the installation folder.

Operation return codes:

While the Common Inventory Technology component is in operation, errors can occur. Use the return code to determine how to resolve any problems that arise.

The table below lists the return codes returned by this component during operation.

Table 45. Common Inventory Technology operation return codes

Return code	Return value	Description
1	WSRC_WRONG_PARMS	At least one parameter is incorrect.
2	WSRC_INPUT_FILE_PARSE_ERROR	An error occurred while parsing the configuration file.
3	WSRC_SIGNATURE_FILE_PARSE_ ERROR	An error occurred while parsing the signature file.
4	WSRC_OUTPUT_FILE_ERROR	An error occurred while writing the output file.
5	WSRC_INPUT_FILE_ERROR	An error occurred while writing the input file.
6	WSRC_MISSING_SIGNATURE_FILE	No signature file was specified and no default signature file is available.
7	WSRC_VALUE_OUT_OF_BOUND	One of the values you specified exceeds the assigned limits.
8	WSRC_INTERNAL_ERROR	An internal error has occurred.

Table 45. Common Inventory Technology operation return codes (continued)

Return code	Return value	Description
9	WSRC_TIMEOUT_ELAPSED	The specified timeout has expired.
10	WSRC_UPGRADE_IN_PROGRESS	Common Inventory Technology is being upgraded and commands are currently not responding.
11	WSRC_FILE_READ_ONLY	The output file is read only.
12	WSRC_INIFILE_NOT_FOUND	The `cit.ini` file was not found.
13	WSRC_CITFILE_NOT_FOUND	The Common Inventory Technology configuration file was not found.
14	WSRC_CCLOGFILE_NOT_FOUND	The `CitTrace.properties` file was not found.
15	WSRC_KEY_NOT_FOUND	The specified value is incorrect.
16	WSRC_VALUE_NOT_VALID	The specified value is not valid.
17	WSRC_KEY_CANNOT_CHANGE	The specified key cannot be modified.
18	WSRC_FILE_CANNOT_OPEN	The specified file cannot be opened.
19	WSRC_FILE_CANNOT_RENAME	The specified file cannot be renamed.
20	WSRC_FILE_CANNOT_DELETE	The specified file cannot be deleted
21	WSRC_CITFILE_NOT_VALID	The `cit.ini` file is corrupt.
22	WSRC_CIT_TRACEFILE_NOT_ VALID	The trace file is corrupt.
24	WSRC_INVALID_AGE	The specified age is incorrect.
25	WSRC_INVALID_TIMEOUT	The specified timeout is incorrect.
26	WSRC_INVALID_ATTRIBUTE	The specified attribute is incorrect.
27	WSRC_INVALID_OUTPUT_FORMAT	The specified output format is not supported.
28	WSRC_CANNOT_LOAD_PROVIDER	The required .dll or shared library file is not available.
29	WSRC_QUERY_TIMED_OUT	The query has reached the timeout.
30	WSRC_QUERY_FAILED	The query has failed.
31	WSRC_PROCESS_INTERRUPTED	The process was interrupted.
32	WSRC_NO_CONFIG_NAME	No configuration file was specified.
33	WSRC_NO_CONFIG_OPTION	No configuration option was specified.
34	WSRC_NO_OUTPUT_NAME	No output file was specified.
35	WSRC_NO_PARMS	No parameters were specified.
36	WSRC_EMPTY_CONFIG_ELEMENT	The configuration file contains an empty element.
37	WSRC_FAILURE	An internal error occurred.
38	WSRC_NO_SORT_FIELD_NAME	A sort option was specified but no sort criterion was specified.
39	WSRC_INVALID_SORT_FIELD_ NAME	The specified sort criterion is incorrect.
40	WSRC_WARNING_FILE_ERROR	An error occurred while attempting to create the warning file during a software scan.

Table 45. Common Inventory Technology operation return codes (continued)

Return code	Return value	Description
41	WSRC_UNABLE_TO_INITALIZE	The process initialization failed.
42	SRC_MISSING_XSS_SCHEMA_FILE	The signature catalog schema was not found.
45	WSRC_UNABLE_INSTALL_DRIVER	The following drivers cannot be installed: `CITMDRV_IA64.SYS`, `CITMDRV_AMD64.SYS`, `CITMDRV.SYS`.
46	WSRC_UNABLE_LOAD_ CITMEMDLL	The `CITMEM.DLL` library cannot be loaded.
47	WSRC_UNABLE_LOAD_SYMBOL_ IN_CITMEM	The symbols in the `CITMEM.DLL` library cannot be loaded.
48	WSRC_UNABLE_READ_ CITMEMDLL	The `CITMEM.DLL` library cannot be read.
49	WSRC_FILE_ACCESS_DENIED	Insufficient rights to access the file.
50	WSRC_NOT_AUTHORIZED	Insufficient rights to perform the operation.
51	WSRC_FILE_NOT_FOUND	The specified file or directory does not exist.

Common problems and solutions

This section shows you how solve typical problems that might arise with any installation of IBM Tivoli Asset Discovery for Distributed. Many of the potential problems you might encounter are easy to solve by tweaking settings on the server, on your agent computers, or on other servers on your network, such as a proxy server.

Server installation and upgrade problems

This topic explains how to solve some common problems with the server installation and upgrade.

Table 46. Problems and solutions for installation and upgrade

Problem	Potential solution
Aggregation does not start after upgrading the server.	Check if the administration server trace log includes the following text: `Aggregation is prevented from execution, AGGR_REC_BLOCKED parameter set in ADM.CONTROL`If it does contain such text, the aggregation has been blocked. To solve this issue, you have to import the latest software catalog.
Setup file cannot be launched while running the `setupservers.bin` file.	You might not be logged on as the root. Log on again as the root and try again.

Table 46. Problems and solutions for installation and upgrade (continued)

Problem	Potential solution
The installation wizard will not run.	There are several reasons why this might happen: • You do not have administrative privileges to the computer where you are trying to install the product. Ensure that you are logged on as an administrator (Windows) or root (UNIX). • There is not enough disk space to create the necessary temporary files. Check the space available on the computer where you are installing the product. • You are trying to install on a platform that is not supported.
The installation wizard hangs when installing on Linux platforms.	A prerequisite for the Java Virtual Machine (JVM) is missing. Check the JVM prerequisites for the platform on which you are installing. See the Installation section for details.
Installation does not start and a message indicating that there in no supported JVM is displayed. This problem occurs even when the supported JVM is present, when the system response is slow.	This problem is caused by a time out of the InstallShield JVM verification routine. Relaunch the installation using the parameter **-is:jvmtimer <timeout in seconds>**. Specify a reasonably high number of seconds to avoid the time out. For example, start by trying 60 seconds and increase the time if the problem persists.
The installation wizard will not finish.	If one of the last steps in the installation (for example, servers startup or chmod) fails, there might not be enough free memory. Check the log file and look for OutOfMemoryError. In this case you can try freeing memory by: stopping Asset Discovery for Distributed servers; stopping the embedded WebSphere Application Server, and rerun the steps. You should consider that in this case you are at the memory limit and even if you are able to install the product, you can encounter problems when running it. Every Asset Discovery for Distributed server requires at least 770 MB free memory to deploy and 1 GB to run.
A java core dump occurs during installation.	Out of memory errors can occur during the installation of the server causing a Java core dump. If the out of memory condition prevents the installation from completing, increase the available memory to allow the installation to complete. The server requires at least 1GB free to deploy and 3GB to run with the database installed.

Table 46. Problems and solutions for installation and upgrade (continued)

Problem	Potential solution
Installation of the server fails on a Sun workstation.	The following error is reported in the trace: Altering bufferpool SQL20189W The buffer pool operation (CREATE/ALTER) will not take effect until the next database startup due to insufficient memory (SQLSTATE=01657). Causes and solutions: The problem is related to the tuning of the shared memory available for the DB2 database. To solve the problem, increase the value of the shared memory (variable shmsys:shminfo_shmmax).
On Solaris, it is not possible to resume an installation if a reboot is made before resuming the installation.	If you resume an installation after a reboot on Solaris, all content of the `/tmp` directory is deleted during the reboot (it resides in swap memory). If a server installation fails and a reboot is performed before resuming the installation, it is not possible to continue the installation because all temporary files required to resume the installation have been deleted from the `/tmp` directory. If an installation fails on Solaris, do not perform a reboot before you attempt to continue the installation because all temporary files required to resume the installation will have been deleted from the `/tmp` directory. If a reboot is absolutely necessary, you must backup the `/tmp/tad4d72` directory and the `/tmp/trace*` files. Perform the reboot, then restore the directory and the files, then resume the installation.
The installation wizard running in unattended mode on a Windows platform does not recognize the presence of the DB2 server. If the installation wizard is used to install a database together.	This problem occurs if the second installation is performed from the same command window as the first. At the end of the first installation, the command window environment is not updated with the information about the newly installed DB2 server. If a second installation is then performed from the same window, it is unable to identify the presence of the DB2 server. If you run the second installation from a new command window, opened after the installation of the DB2 server has been completed, the problem is resolved.
Installation of a database on a UNIX platform fails when the installation path name includes double-byte characters. The script that creates the database fails to run when the installation path name includes double-byte characters. The database installation log, trace_db_servers.log, shows that the script failed because its path could not be interpreted. The path shown in the log file is garbled.	This problem occurs when the environment settings on the target computer are set incorrectly. Settings required to run scripts are obtained from the /etc/environment file. It is probable that this file includes the setting: LC_MESSAGES=C@lft. This setting restricts the characters that can be used in the environment to the ISO 8859-1 (ASCII) character set, and so double-byte characters cannot be used. To resolve this problem, comment out the LC_MESSAGES=C@lft setting and rerun the installation.

Table 46. Problems and solutions for installation and upgrade (continued)

Problem	Potential solution
Installation of a database on a UNIX platform fails during the "Creating and populating the administration server database" phase. The `trace_db_servers.log` file shows that shared memory settings could not be allocated.	The shared memory settings are not sufficient. See the user documentation for your system for information about how to increase the shared memory size.
Installation fails because of a problem with temporary storage space.	The installation requires some free space in the /tmp directory and will fail if this space is not available. For more information, view the space requirements. If you cannot clear sufficient space in the /tmp directory, you can specify an alternative temporary file storage location when you launch the setup command. The syntax is: `setupservers.bin -is:tempdir <TEMP_DIR>`.
No result record for a step in the Resume Installation panel.	If some invalid characters are present in the command STDOUT or STDERR, the installation will fail to create the result record associated with the failed step. In this situation the command standard output and command standard error is written to the log file and a dummy entry placed in the result record associated with the step. The information that is written to the log file can be used to diagnose the problem.
Installation fails because there is not enough disk space.	This is a known installation wizard problem, and also occurs during a silent installation. On AIX® systems the disk partitions are resized at runtime to accommodate the additional space requirements. The installation wizard caches the file system information when it starts, and it does not update this information while the install program is running. This can cause two effects: • The preview panel may claim that more space is needed than what is currently available (the preview panel however will also display the message: ⌂The following file systems will be expanded during the installation⌂. • Because the disk space check is performed using cached information there is a possibility that disk space check operations will claim that there is enough space even when not enough space is available.

Table 46. Problems and solutions for installation and upgrade (continued)

Problem	Potential solution
The server installed on an AIX platform does not start.	This problem is caused by a conflict of ports used by WebSphere Application Server. The problem and its workaround are documented in the Redbook: IBM WebSphere Application Server, version 5.0 System Management and Configuration, SG24-6195. Refer to sections 6.6.2 and 6.7.2, which deal with IP port conflicts. You can access the IBM redbooks publications from the following site: http://www.redbooks.ibm.com.
The server installed on a Windows platform does not start.	This problem occurs when the server has been uninstalled prior to the installation, and the uninstallation has failed to complete the deregistration of the old server, so it is still pending. To resolve the problem of the pending deregistration, you must restart the computer. The new server can now be registered. You can do this as follows: 1. Open the file <*SERVER_INSTALL_DIR*>\admin\setup\setupAdmin.bat. 2. Copy the last line of the file and paste it into the command window. 3. Run the command.
When reinstalling Tivoli Asset Discovery for Distributed server or database (or both) that have been uninstalled, it is (or they both are) grayed out and cannot be selected.	The problem occurs because the appropriate entries have not been removed from the vital product data (VPD) registries. Tivoli Asset Discovery for Distributed uses its own dedicated copy of VPD registries. It is located in the `ITLCM-SERVER` directory. The exact location of this directory depends on the operating system: • `/usr/lib/objrepos/common` (AIX) • `/home_directory/common` (HP-UX) • `/home_directory/common` (Linux) • `/InstallShield/Universal` (Solaris) • `\Program Files\InstallShield\Universal\Common Files` (Windows) To resolve this situation, locate the directory `ITLCM-SERVER` and remove it.

Table 46. Problems and solutions for installation and upgrade (continued)

Problem	Potential solution
The server installation wizard displays the information that there are components already installed even though the files have been removed from the file system.	The problem occurs because the appropriate entries have not been removed from the vital product data (VPD) registries. Tivoli Asset Discovery for Distributed uses its own dedicated copy of VPD registries. It is located in the `ITLCM-SERVER` directory. The exact location of this directory depends on the operating system: • `/usr/lib/objrepos/common` (AIX) • `/home_directory/common` (HP-UX) • `/home_directory/common` (Linux) • `/InstallShield/Universal` (Solaris) • `\Program Files\InstallShield\ Universal\Common Files` (Windows) To resolve this situation, locate the directory `ITLCM-SERVER` and remove it.
When the browser opens at the end of the installation of a server, the logon page of the Web UI is not found.	This can occur if the administration server has not correctly plugged in to WebSphere Application Server. To resolve the problem, you must regenerate the Web server plugin configurations. To do this, complete the following steps: 1. Start the WebSphere Administrator's Console. 2. In the navigation pane, click Environment Update Web Server Plugin. 3. On the page that is displayed, click **OK**. 4. Stop and restart the administration server.
Following installation of a server on a UNIX platform, an attempt to log on to the server Web UI fails with a server initialization error.	This problem is caused by the failure of the installation wizard to create the tlmsrv user during the installation of the database. The reason for this failure is that the adduser command is not included in the `$PATH` variable. To resolve the problem, use the adduser command to create the tlmsrv user on the computer where the database is installed. To avoid this problem happening again, ensure that the adduser command is included in the `$PATH` on all computers where you are planning to install a database.
During the installation of a server on a UNIX platform, the tasks related to the creation of the databases fail and result in error.	The step related to creating the databases results in error if the DB2 services are not running at the time of installation. The install wizard allows you to pause the installation, diagnose the problem, and run the failed step again. Refer to IBM Tivoli Asset Discovery for Distributed: Planning, Installation, and Configuration, SC32-1431 for more information about resuming a failed installation. To solve the problem, start the DB2 services and resume the installation.

Table 46. Problems and solutions for installation and upgrade (continued)

Problem	Potential solution
Installation fails on UNIX because of the umask settings.	Installation is not allowed to change system umask or force permissions to file systems such as `/opt` or `/usr`. Before you install, make sure that sufficient permissions are set on any subdirectories in file systems such as `/opt` or `/usr`. You must ensure that the DB2 administrator (typically `db2inst1`) has sufficient permissions to run scripts on this file systems (at least 755).
Installation ends successfully but the server cannot be reached through the HTTP server.	On Windows, the WebSphere installation path and node name can be combined in a way that the Web server configuration fails because path names exceed the Windows limit. As a result, Asset Discovery for Distributed works only on WebSphere Application Server internal transports. Reinstall WebSphere Application Server shortening the path, then re-install Asset Discovery for Distributed.
Installation fails when started from a local machine.	If the installation of the server or the catalog manager is not initiated from the CD, but from a copy on the local machine, ensure that the path to the set up file does not contain special characters (for example, an exclamation mark), otherwise, the installation fails with an error. The following is an example of a path containing a special character: `C:\!Installation\TLM\setup\servers\setupServers.exe`
While uninstalling the server, the Java process of the bundled WebSphere Application Server remains alive.	To uninstall the server, you must use the following files: `installLocation/cli/srvstart.bat` & `srvstop.bat`. Do not use the bundled WebSphere Application Server files: `startServer.bat` or `stopServer.bat` in the `eWAS` directory.
When installing the server into an existing database server infrastructure, the installer does not recognize the password for the `tlmsrv` account (which is created automatically during installation).	This could happen for different reasons: On Linux servers, if PAM (Pluggable Authentication Module) is not installed, you must install it. For HP Unix trusted systems (according to Websphere Application Server - Express, Version 6.0.x documentation) If you are using the local operating system user registry, HP-UX must be configured in untrusted mode. Trusted mode is not supported if global security is enabled using the local operating system user registry. See the following link for more information: http://publib.boulder.ibm.com/infocenter/wasinfo/v6r0/index.jsp?topic=/com.ibm.websphere.express.doc/info/exp/ae/csec_localos.html

Table 46. Problems and solutions for installation and upgrade (continued)

Problem	Potential solution
Server installation fails and the install log indicates that a DB2 command cannot be found. This could happen on AIX and Solaris computers, or UNIX systems in general.	Stop the installation and run the following: `. ~db2inst1/.profile`. Restart the installation using `-resume` switch. If the shell is set to `/usr/bin/bash` change the **db2inst1** user's default shell to `/usr/bin/ksh`.
When installing the server with DB2 on computers running Windows Server 2008, the installation of the database fails.	You must obtain DB2 DB2 9.1 Fix Pack 4 to install on Windows Server 2008 machines.
On the Solaris 10 SPARC server, installation fails during creating and populating the server. The `trace_db_servers.log` file contains the following message: `SQL1478W The defined buffer pools could not be started. Instead, one small buffer pool for each page size supported by DB2 has been started. SQLSTATE=01626.`	The installation failed because kernel parameters on Solaris had not been set. The output from the db2osconf script in the DB2 installation directory shows the parameters with values that need to be set to allow the database to function properly. You can set these parameters in the `/etc/system` file. When you have set the parameters, restart the system and repeat the installation process.
On UNIX systems, when installing the server in interactive mode without graphical interface, the following message appears: `The installer is unable to run in graphical mode. Try running the installer with the -console or -silent flag.`	The `-console` option is not supported. If you run the installer with this option, an error will occur. To install the server in interactive mode on UNIX and Linux machines, there must be graphical interface available. Otherwise, you must use silent mode.
Problem with data sources initialization. The following errors occur: • An error message on Home page: `An error that prevented the system from accessing the database occurred.` • If you use **Test connection**, you get an error message on License Metric Tool DataSource window: `The test connection operation failed for data source LMT DataSource on server server1 at node NC143014Node02 with the following exception: java.sql.SQLException: [ibm][db2][jcc][t4][10205][11234] Null userid is not supported.DSRA0010E: SQL State = null, Error Code = -99,999. View JVM logs for further details.` • An error message with the ID CODDB3008E in the `<TCD>/logs/admin/messge/msg.log` file.	Restart the server.
The installation fails and the following message appears in the log file: `java.io.IOException: Not enough space at java.lang.UNIXProcess.forkAndExec(Native Method).`	The installation failed because of lack of memory. Increase the available memory to allow the installation to complete. **Remember:** Close all running programs before you start the installation.

Table 46. Problems and solutions for installation and upgrade (continued)

Problem	Potential solution
The connection with the database cannot be established despite the fact that the values specified for the tlmsrv user, host name and port number are correct. The *temp_dir*/tad4d contains the following error message: `A SQLException caught: java.net.ConnectException : Error opening socket to server <db2_host> on port <db2_port> with message : Connection timed out DB2ConnectionCorrelator: null.`	Try to connect to the database using the DB2 client to find out more about the problem.
Asset Discovery for Distributed Launchpad cannot be started on Unix platforms.	When starting the Asset Discovery for Distributed Launchpad from the hard disk of your Unix computer, ensure that the path to the launchpad executable file (`launchpad.sh`) does not contain spaces.
When installing on AIX, if you free disk space in one of the directories used during installation, the installation wizard does not refresh the space information.	Restart the installation wizard.
When installing on Solaris or HP-UX operating systems, creating and populating the administration server database fails and the following error occurs: `CODIN0035E An error occurred while populating the administration server database.`	The installation failed because of wrong **shmmax** parameter value. Use the db2osconf command to identify proper settings for this parameter. See the DB2 information center for more information: http://publib.boulder.ibm.com/infocenter/db2luw/v9/index.jsp?topic=/com.ibm.db2.udb.admin.doc/doc/r0008113.htm.
When upgrading License Metric Tool from V7.1 to V7.2 the server upgrade and database migration procedures complete correctly but the following information is displayed: `CODIF0014I Database version is higher than expected.` The error is recorded in the Message Handler log.	The situation happens if License Metric Tool 7.1 database is migrated before the server is upgraded to V7.2 (the database does not match the code version). The error may appear at the beginning of the upgrading procedure when the installer starts the WebSphere Application Server to verify if security has been set. The recommended solution is to ignore the information and proceed with the upgrade.
When installing the **tlma** database component the installer fails and the CODIN0154E message is displayed: `The directory /tmp has not the required permissions set or the database instance owner is not valid.`	If your DB2 instance owner home directory does not follow the pattern `<unix_home_dir>/<db2_instance_owner_name>`, create a symbolic link that will point to the DB2 instance owner home directory and select this symbolic link as an instance owner name during the installation. Example: If your DB2 instance owner is **db2inst1** and its home directory is `/home/db2`, the installation will take **db2** as the instance owner name. To fix it, create a symbolic link with `/home/db2inst1` pointing to `/home/db2` directory and then use `/home/db2inst1` as the instance owner home directory in the installation wizard.

Table 46. Problems and solutions for installation and upgrade (continued)

Problem	Potential solution
After upgrading the License Metric Tool 7.1 or License Compliance Manager 2.3 server to Asset Discovery for Distributed V7.2, the agents cannot communicate with the server.	The problem may have occurred because of a change in Asset Discovery for Distributed V7.2 communication settings. The License Metric Tool 7.1 and License Compliance Manager 2.3 server with security level set to Medium is able to communicate with agents with security set to Minimum. In Asset Discovery for Distributed 7.2 it is no longer possible. Therefore, ensure that the security level set on V7.2 agents is the same or higher than that of the upgraded server.
Server installation fails on Solaris 10 SPARC platform during the creating and populating of the database. The following message is recorded in trace_db_servers.log file: `SQL3306N An SQL error "-1218" occurred while inserting a row into the table. SQL1218N There are no pages currently available in bufferpool "4096".`	The problem may be caused by DB2 V9.1 or 9.5 self-tuning memory mechanism. It can be resolved by the installation of the latest DB2 fix pack. If the problem persists, disable Self-Tuning Memory Manager and configure DB2 manually. For more information refer to http://publib.boulder.ibm.com/infocenter/db2luw/v9r5/index.jsp?topic=/com.ibm.db2.luw.admin.config.doc/doc/r0006017.html .

While upgrading the Asset Discovery for Distributed server from Tivoli License Compliance Manager V2.3 fix pack 6 an error occurs and the CODIF6011E message is displayed:
 	
`Message text: The connection to the database could not be initialized.`
 	
`Explanation: Either at least one database pooler configuration parameter is missing or incorrect, or the password used by the server to access the database is incorrect.`
 	
`User response: Check that the database is available. If it is, ensure that configuration settings for accessing the database are correct: Check the host name and port properties defined in the db.properties file on the server computer. Check that the data source for the server has been correctly defined on WebSphere Application Server. Ensure that the password held on the server computer is aligned with the password of the tlmsrv user on the database computer. The password held on the server computer is changed using the dbpasswd command from the server CLI. The database configuration, including the JDBC resources is correct.`
	The problem may occur during the stopping and starting of the Tivoli License Compliance Manager administration or runtime server on Linux operating system. The error is caused by the embedded WebSphere Application Server V6.1 exchanging its internal SSL certificates because of their expiration. As a result of this the files in the following directories *profiledir*`/config/cells/cellname/.../*.p12` and *profiledir*`/etc` may have different timestamps (the files in the `etc` directory might be older), which means that the replacing of certificates has not been successful.
	
	Make a backup copy of the certificate files before you start the upgrade procedure and replace the files in the `profiledir/etc` folder with the backed, valid certificate files if the problem has occurred.

Table 46. Problems and solutions for installation and upgrade (continued)

Problem	Potential solution

While installing Asset Discovery for Distributed on AIX 6.1 with DB2 9.1, a DB2 installation error occurs. The <Tivoli Common Dirrctory>/COD/logs/install/trace/DB2install.log file contains information on minor DB2 installation error:
`ERROR:mkdev: 0514-519 The following device was not found in the customized device configuration database: name = 'aio0'`
 	
`ERROR:An error occurred while enabling Asynchronous I/O. DB2 requires Asynchronous I/O to be enabled to function properly. Enable this manually using "smit aio". If the problem persists contact a technical service representative.`
	Select the step "Installing DB2" as successful and continue the installation.

Agent installation and upgrade problems

This topic explains how to solve some common problems while installing and upgrading the agent.

Table 47. Problems and solutions for agent installation and upgrade

Problem	Potential solution
After upgrading the server, it is not able to answer the requests made by the agent.	Upgrade the agent manually.
On Windows, the agent self-update fails with the -510 return code.	Check if the path located in the `tlmagent.ini` file includes some spaces. If it does, modify the path so that it does not include any spaces, and restart the agent.
The installation wizard hangs when installing on Linux platforms	When a prerequisite for the Java Virtual Machine (JVM) that is bundled with the installation package is missing, check the prerequisites for the JVM on that platform. When you launch the set up file, a Java Runtime Environment (JRE) is installed that is needed by the wizard. Some environmental settings or fix packs might be required to enable the JRE function correctly. Refer to the following information for details of settings and fix packs that are required on each platform: • AIX: IBM developer kits: IBM 32-bit SDK for AIX, Java 2 Technology Edition, Version 1.4 User Guide. • Linux platforms: IBM developer kits: IBM Runtime Environment for Linux Platforms, Java 2 Technology Edition, Version 1.4.2 User Guide. • HP-UX: http://www.hp.com/products1/unix/java/patches/index.html • Solaris: http://sunsolve.sun.com/pub-cgi/show.pl?target=patches/J2SE

Table 47. Problems and solutions for agent installation and upgrade (continued)

Problem	Potential solution
Agent files cannot be downloaded.	This is a network connectivity problem that can be caused by an unusually high amount of traffic or by an agent installation tool error. Wait for a short time and then retry the operation. If the problem persists, report the problem to the system administrator. Try deploying the agent from a different machine.
No status is returned to the server.	Check that the agent has been installed on the node. On Windows, you can open the services panel from the control panel and check for the agent. On UNIX, enter the following command: `ps -ef | grep tlmagent`. If the agent is running a response is returned. If it is not, there is no response. Also check the `slmrc` file for the return code.
Agent installation fails on Red Hat Enterprise Linux version 4 The agent installation fails and in the install agent trace the following error is displayed: `wdinstsp: error while loading shared libraries: libstdc++.so.5: cannot open shared object file: No such file or directory`	Install the following compatible library package: `compat-libstdc++-33-3.2.3-47.3.i386.rpm`
The agent install wizard for i5/OS displays Message CODIN0099E, indicating that the agent cannot be installed. This message indicates that an agent is already installed on the computer	On i5/OS platforms, you must uninstall the agent before reinstalling it. If the objective of the new installation is to change the agent parameters, before you reinstall you must also manually remove the configuration file from the path: `/QIBM/UserData/QITLM/conf` When you reinstall the agent, a new agent ID is generated, so previous information collected by the agent on the computer is not included in any reports for the new agent. The entry for the old agent is still present in the administration server database and cannot be immediately deleted. Agents must be recognized by the administration server as inactive before they can be deleted. When the agent status changes to inactive, you can delete it.
Following automatic self-update on Windows platforms, the agent does not restart automatically.	The agent does not restart because a reboot of the computer is needed to load libraries required by the corequisite GSkit software.
Agent self-update fails because a security certificate cannot be added to the agent keystore.	Agent self-update can be triggered by a change to the agent itself of a change to its security certificate. If the update is required because of a changed certificate you must ensure that the certificate has not already been changed on the current date. When certificates are automatically imported into the keystore the day, month, and year of the import is assigned as the unique ID of the certificate, so only a single import can be allowed on any one day.

Table 47. Problems and solutions for agent installation and upgrade (continued)

Problem	Potential solution
A certificate for secure communications is not added to the keystore.	This happens if a certificate has already been added to the keystore on the same day. Only one certificate can be added automatically on any one day. You can either add the certificate manually using the keystore utilities or wait until the following day for the automatic update to be performed. Run the following command: **setagentconf -s active**
Agent installation fails on Linux 390 platforms with the **error -8** in the log file `/tmp/manualDeploy/tmp_dir/slmrc` and in the trace file, the following entry appears: `<LogText><![CDATA[WizardException: (error code = 200; message="Unable to find success string in the log file: /tmp/manualDeploy/tmp_dir/slmrc")]]></LogText>`	Verify that you entered the correct values for **Shared pool capacity** and Active processors.
Unable to uninstall the agent (manual Websphere Application Server installation used) on computers running Windows Vista (32 bit). The agent does not appear in the "Programs to remove" list.	Uninstall the agent with the `tlmuninst` script. See the *Installation Guide* for details.
Agent installation fails if the agent was previously installed and uninstalled.	In order to do a fresh installation of agent the following files and directories must be deleted prior to the installation: • `/etc/tlmagent.ini` • `/var/itlm/` • `/.swdis/5724-D33` File paths and names can differ in case of custom installation.
You cannot put the focus in entry fields using Cygwin/X as a remote X-server after displaying the modal window. This happens when you forget to enter server information during the install and you try advance to the next screen. An error message tells you that you must enter server information, but then you will not be able to put the focus of the cursor in any text fields.	To solve this problem, launch the X-server using the Cygwin/X `startx` command as it is suggested at the following link: http://x.cygwin.com/docs/ug/using.html.

Table 47. Problems and solutions for agent installation and upgrade (continued)

Problem	Potential solution
The agent does not start on Linux systems (such as zLinux) and the following message appears: **CODAG016E** - An error occurred starting the agent. Check for messages like the following: SELinux is preventing `/opt/tivoli/cit/bin/wscancfg` from loading `/opt/tivoli/cit/bin/libbase.so` which requires text relocation. You can find SELinux logs in the **syslog** in `/var/log/messages`. To view complete SELinux messages, run the following command: **`sealert -l d601071f-34fe-4ef4-ad97-2dada2900635`**.	This error occurs when your Linux operating system is in **Enforcing** mode. You must change the mode to **Permissive** or **Disabled** before you install the agent. To do so, set the parameter `SELINUX` in the file `/etc/selinux/config` to **`permissive`** or to **`disabled`**. You cannot set the security setting back to **Enforcing**; if you do so the agent will stop working. **Enforcing** mode may be preserved if you decide to change the file context to `textrel_shlib_t` for all the libraries used by agent using the command: `chcon -t textrel_shlib_t /path_to_lib/libname.so`
On AIX, the native installer hangs after installation. The agent is installed successfully, but the status is not changed to success. The following message is displayed: `Some entries in the next screen do not have the correct string length. Check your language environment variable and the code set.`	This error occurs when the packages `bos.loc.com.utf` and `bos.loc.utf.EN_US` are installed on the system, and the **LANG** environmental variable is set to **EN_US**. Change the value of the **LANG** variable in `/etc/environment` from **EN_US** to **en_US**, or type `LANG=en_US` to change the value for the current session only.
On AIX, after upgrading the server from version 7.1 to 7.2 you may experience a situation when the agent version 7.1 stops sending scheduled software scans.	To solve this problem, stop the agent, delete its cache and start the agent.
The agent cannot be uninstalled by system native installation tools after it has been upgraded from version 2.3 or 7.1 to 7.2 using Tivoli Configuration Manager or the self-update method. System registry is not updated.	On an agent upgraded in this way a refresh installation using native installation method can be performed. In this case, system registry will be updated. After that, you can uninstall the agent using the `tlmunins.sh` script.

Table 47. Problems and solutions for agent installation and upgrade (continued)

Problem	Potential solution
If an agent running in an AIX 6.1 *logical partition* (LPAR) is upgraded to version 7.2 using Tivoli Configuration Manager or self-update method, it might be impossible to install version 7.2 agents in *workload partitions* (WPARs) created in the logical partition (LPAR).	There are two ways to install the agent in a workload partition: • Reinstall the agent in the logical partition using native installation method and then install agents in workload partitions using native installation methods, too. • Do not change the configuration of the agent installed in the logical partition but perform the installation in workload partition paying special attention to the paths in the response file. To install the agent in a workload partition, perform the installation in the same way as in the logical partition but provide all paths in the response file, ensuring that no directory that is shared with global AIX is read only. In particular, Common Inventory Technology installation directory needs to be modified since the default is located under the `/opt` directory, which for default workload partition is set to read only.
After upgrading a version 2.3 Tivoli License Compliance Manager agent on a pSeries logical partition, the Classify Relocation panel contains record for upgraded agent even though relocation has not taken place (in a typical upgrade situation the Classify Relocation panel remains empty).	This situation occurs because the agent on p-Series logical partitions reports a virtualization hierarchy differently than Tivoli License Compliance Manager v2.3. For this reason an agent upgrade is always treated as a change in virtualization configuration and presented on the Classify Relocation panel. This relocation is reported on the date of agent (not server) upgrade, and therefore can be spread over time. This does not affect the values present in the audit report.
Fix Pack 1 Uninstallation of version 7.2. FP 1 agent may fail if the agent was update from the GA level.	If you are running the uninstaller in graphical mode, you are given the option to force uninstallation. Otherwise, remove the `%HOMEDRIVE%\swdis\5724-D33` directory on Windows or `/.swdis/5724-D33` on UNIX once the uninstaller finishes.

Validating and troubleshooting server installation

This section explains how to validate that the server has been successfully installed.

You can access the Integrated Solutions Console, which contains the IBM Tivoli Asset Discovery for Distributed console, at the following URL: `http://`*`administration server IP address`*`:8899/ibm/console/login.do`. If you cannot access the console, follow the procedures in this section.

For server-specific return codes, see the "Server information" on page 125 section.

Checking the command line and Web server

Check the server command line and the Web server if you cannot access the Tivoli Asset Discovery for Distributed console.

1. To check the command line, perform the following actions:
   a. On the administration server computer, open the command line (on Windows go to **All Programs → Asset Discovery for Distributed →**

Administration server command line, on Linux or UNIX run <*SERVER_INSTALL_DIR*>/cli/lmtcli.sh).

b. Enter the following command: `info`.

This command should return the following information:

- The version installed.
- The install path.
- The name of the DB2 database for the server.
- Build version.

Note: To run this command, the security must be turned on and the user has to be logged in.

2. To check the Web server, perform the following actions:
   a. Open a browser window.
   b. Enter the following URL: `http://<HOSTNAME>:8899/ibm/console/`.

   The Welcome page with login box opens. If it does not, see the *Server installation and upgrade problems* section of the infocenter for troubleshooting suggestions.

Ensuring the server is started

Use the Websphere serverStatus command to check if the server is working.

Before you begin

You need to be logged in as a user with administrative rights (root on UNIX and Linux platforms, or Administrator on Windows).

1. Run the script serverStatus.sh (UNIX) or serverStatus.bat (Windows) available in the WebSphere Application Server bin directory: <*TADD_INSTALL_DIR*>\eWAS\bin.
2. If the server has not been started, start it by running the script srvstart.sh (UNIX) or srvstart.bat (Windows).
3. If the server fails to start and an exception message informs you that the HTTP transport port is in use, do the following:
   a. Release the port number.
   b. Restart the HTTP server and the administration server for the changes to take effect.

Chapter 3. Configuring Tivoli Asset Discovery for Distributed

You need to perform some configuration tasks during and after the upgrade.

Configuring the Tivoli Asset Discovery for Distributed server

After the Tivoli Asset Discovery for Distributed server is installed, you need to enable the security and configure access rights for users.

Starting the server

When you are starting the server, you also need to start the DB2 database software.

Note: DB2 must be started before the server.

1. Start the DB2 instance. Note you can set up DB2 to autostart after each system restart. This is the default setting for DB2 instances created during installation on the Windows operating system. If DB2 is not set up to autostart:
   a. Log into DB2 with the DB2 administrator ID and password specified at installation time.
      - On UNIX platforms, you need to run the following startup script after logging in:
        `$INSTHOME/sqllib/db2profile`
   b. Type `db2start` at a command line.

   The DB2 instance starts.
2. Go to the directory <*INSTALL_DIR*>/cli, where <*INSTALL_DIR*> is the name of the Tivoli Asset Discovery for Distributed installation directory.
3. Run the script srvstart.bat (Windows) or srvstart.sh (Unix).
   - You can also start the server by entering the `srvstart` command at the Asset Discovery for Distributed command-line interface. If security is enabled, you will be prompted for an administrator user ID and password.

The server starts.

Stopping the server

When you are stopping the server, you might also consider stopping the DB2 database software.

1. Go to the directory <*INSTALL_DIR*>/cli, where <*INSTALL_DIR*> is the name of the Tivoli Asset Discovery for Distributed installation directory.
2. Run the script srvstop.bat (Windows) or srvstop.sh (Unix).
   - You can also stop the server by entering the `srvstop` command at the Asset Discovery for Distributed command-line interface. If security is enabled, you will be prompted for an administrator user ID and password.

   Note: On Linux and Unix, when security is turned on, either the X server must be available, or the **-username** and **-password** parameters must be used. For more information on the parameters, see ../com.ibm.license.mgmt.commands.doc/srvstop.dita.
   The server stops.
3. Additionally, you may want to stop the DB2 instance.

a. Log into DB2 with the DB2 administrator ID and password specified at installation time.
b. Type `db2stop` at a DB2 command line.

The DB2 instance stops.

Enabling and configuring server security

It is important to enable and configure security on the Tivoli Asset Discovery for Distributed server, as the application is not secured by default.

1. Log into the Integrated Solutions Console. No authentication is required.
2. Expand the **Security** group and navigate to the **Secure administration, applications, and infrastructure** panel.
3. Click **Security Configuration Wizard**.
4. Check **Enable application security**.
5. In the next panel, choose the user repository.
6. Configure server security.

Restart theTivoli Asset Discovery for Distributed server and log into the console using your administrator credentials defined in this task.

Configuring permissions for users

After you have enabled security for the Tivoli Asset Discovery for Distributed server, you need to configure access rights for the users. You can do this by assigning user to roles, for example *Inventory administrator*.

1. Log into the Integrated Solutions Console using the credentials defined in *Enabling and configuring Tivoli Asset Discovery for Distributed server security*.
2. Expand the **Users and groups** section of the navigator and click **Administrative User Roles**.
3. Click **Add**. A new screen opens.
4. Type in the new user's login in the **User** field.
5. Choose the user role from the **Role(s)** list. It is possible to assign multiple roles to a user by holding the Ctrl key and selecting the appropriate items.
6. Click **Apply** to save the changes, or **OK** to save and close.

Conducting Network Scan

Network Scan is a process which aims at discovering computers which are active in your network and on which Tivoli Asset Discovery for Distributed agents have not been installed. The scan imports a file with details about your infrastructure, and then compares it with information about the agents connected to this particular server.

Before you begin

To aid in the identification of operating systems, you can specify a minimum confidence level for operating systems found by the discovery engine through the **discoveryMinConfidenceLevel** parameter in the `system.properties` file. Any operating systems with a confidence level lower than the value specified will not be displayed in the Network Scan Details pane in the Tivoli Asset Discovery for Distributed web interface. Specifying a value of zero will cause all discovered operating systems to be taken under consideration.

1. To discover new machines in your infrastructure, as well as information about their operating systems, run an external application for scanning networks (for example Nmap).
   - You can also run a script or other program which lists the machines in your network on the basis of the output from a DHCP server (IP tables), or prepare the list of computers manually.
2. Prepare a `<filename>.xml` file which contains the information about your network, either manually or using an automated tool. The schema of the file should be identical with the one provided by IBM. See *Definition for network discovery scans* for detailed information about the structure of the file.
3. Enter the following command into the command-line interface to import the XML file into the Tivoli Asset Discovery for Distributed server database:

   ```
   impnetscan -f <path_to_the_file>
   ```

   The `-f` parameter is mandatory.

   For details about the impnetscan command, see the "Commands" section of the information center.

Definition for network discovery scans

This topic describes the format for the network discovery scan XSD.

The XML definition for network discovery scans has the following format:

```
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema" elementFormDefault="qualified" attributeFormDefault="unqualif

 <xs:element name="nmaprun">
  <xs:complexType>
   <xs:sequence>
    <xs:annotation>
       <xs:documentation>
        This element should be a root element and it should contain at least one 'host' element.
       </xs:documentation>
    </xs:annotation>
    <xs:any processContents="lax" minOccurs="0" maxOccurs="unbounded"/>
   </xs:sequence>
   <xs:anyAttribute processContents="lax"/>
  </xs:complexType>
 </xs:element>

 <xs:element name="host">
  <xs:complexType>
   <xs:sequence>
    <xs:element name="status" minOccurs="0" maxOccurs="1"></xs:element>
    <xs:element ref="address" minOccurs="1" maxOccurs="1"></xs:element>
    <xs:choice minOccurs="0" maxOccurs="unbounded">
     <xs:element ref="hostnames"></xs:element>
     <xs:element ref="address"></xs:element>
     <xs:element ref="os"></xs:element>
     <xs:element name="ports"></xs:element>
     <xs:element name="uptime"></xs:element>
     <xs:element name="smurf"></xs:element>
     <xs:element name="distance"></xs:element>
     <xs:element name="tcpsequence"></xs:element>
     <xs:element name="tcptssequence"></xs:element>
     <xs:element name="ipidsequence"></xs:element>
     <xs:element name="times"></xs:element>
    </xs:choice>
   </xs:sequence>
   <xs:anyAttribute processContents="lax"/>
  </xs:complexType>
 </xs:element>

 <xs:element name="address">
  <xs:complexType>
   <xs:attribute name="addr" type="xs:string" use="required"/>
   <xs:attribute name="vendor" type="xs:string" use="optional"/>
   <xs:attribute name="addrtype" use="required">
    <xs:simpleType>
     <xs:restriction base="xs:string">
```

```
      <xs:enumeration value="ipv4"/>
      <xs:enumeration value="ipv6"/>
      <xs:enumeration value="mac"/>
     </xs:restriction>
    </xs:simpleType>
   </xs:attribute>
   <xs:anyAttribute processContents="lax"/>
  </xs:complexType>
 </xs:element>

 <xs:element name="hostnames">
  <xs:complexType>
   <xs:sequence>
    <xs:element name="hostname" minOccurs="0">
     <xs:complexType>
      <xs:attribute name="name" type="xs:string" use="required"></xs:attribute>
      <xs:attribute name="type" type="xs:string" use="optional"></xs:attribute>
     </xs:complexType>
    </xs:element>
   </xs:sequence>
   <xs:anyAttribute processContents="lax"/>
  </xs:complexType>
 </xs:element>

 <xs:element name="os">
  <xs:complexType>
   <xs:sequence>
    <xs:element name="portused" minOccurs="0" maxOccurs="unbounded"></xs:element>
    <xs:element name="osclass" minOccurs="0" maxOccurs="unbounded">
     <xs:complexType>
      <xs:attribute name="type" type="xs:string" use="optional"></xs:attribute>
      <xs:attribute name="vendor" type="xs:string" use="required"></xs:attribute>
      <xs:attribute name="osfamily" type="xs:string" use="required"></xs:attribute>
      <xs:attribute name="osgen" type="xs:string" use="optional"></xs:attribute>
      <xs:attribute name="accuracy" type="xs:integer" use="required"></xs:attribute>
     </xs:complexType>
    </xs:element>
    <xs:element name="osmatch" minOccurs="0" maxOccurs="unbounded">
     <xs:complexType>
      <xs:attribute name="name" type="xs:string" use="required"></xs:attribute>
      <xs:attribute name="accuracy" type="xs:integer" use="required"></xs:attribute>
      <xs:attribute name="line" type="xs:string" use="optional"></xs:attribute>
     </xs:complexType>
    </xs:element>
    <xs:element name="osfingerprint" minOccurs="0" maxOccurs="unbounded"></xs:element>
   </xs:sequence>
   <xs:anyAttribute processContents="lax"/>
  </xs:complexType>
 </xs:element>

</xs:schema>
```

Table 48 describes the XML elements for the nodes DTD.

Table 48. Deployment element descriptions

Element	Description
nmaprun	Specifies the identifier for the entity.
host	Specifies the discovered entity (e.g. a computer, printer or phone). The required attributes are: **status** Indicates if the entity is up and running. **address** Specifies the IP address of the entity in a given network.

Table 48. Deployment element descriptions (continued)

Element	Description
address	Specifies the IP address of the discovered entity. Required attributes: **addr** Specifies the IP address of the entity in a given network. **addrtype** Specifies the type of the address of the entity in a given network. Possible values are ipv4, ipv6 or MAC address.
hostnames	Specifies the hostname of the discovered entity. Required attribute: **name** Specifies the unique name of the entity in a network.
os	Specifies the name of the operating system. Required (and important) attributes: **vendor** Specifies the manufacturer of the operating system. **osfamily** Specifies the type of the operating system (e.g. Windows or Unix). **osmatch** Indicates if the discovery of operating system is correct. **name** Specifies the exact name of the operating system (e.g. SUSE Linux Enterprise Server 10). **accuracy** Specifies the degree to which the discovery of operating system is correct. The value can be between 0 and 100 (it is 100 when it is certain that a given operating system is installed on a computer). The figure is expressed as a percentage.

Configuring event notifications

You can configure the server to generate email notifications of significant licensing and system administration events. The notifications are then sent to recipients that you select in the Web interface.

You can configure event notifications using the `system.properties` file. For details of the types of notification that can be generated on the server, see the "Troubleshooting and support" section of the information center.

1. Open the`system.properties` file.
   - If the server was installed on the bundled version of WebSphere Application Server, the file is located at `<INSTALL_DIR>/eWAS/systemApps/isclite.ear/tad4d_admin.war/WEB-INF/conf`.

- For the stand-alone version of WebSphere Application Server, the file is located at <*INSTALL_DIR*>WebSphere/AppServer/systemApps/isclite.ear/tad4d_admin.war/WEB-INF/conf.

2. Specify the following parameters:

   smtpServer
   The IP address of your SMTP server.

   mailSender
   The e-mail address from which the notifications will be sent.
3. Restart the server.
4. Log into the Integrated Solutions Console as an administrator.
5. In the navigator pane, select **Tivoli Asset Discovery for Distributed** → **Administration** → **Manage Notifications**.
6. Select **Add Subscriber** from the dropdown list, and click **Go**.
7. In the Add Notification Subscriber page, specify the recipient of notification e-mails, and the events to which they are assigned.
8. Click **OK** to save and close, or **Save and Add Another** to add another recipient.

Moving a database

You can move the Tivoli Asset Discovery for Distributed server database to a different computer to speed up the working of the server.

If your environment has grown after you first installed Tivoli Asset Discovery for Distributed, the larger number of agents reporting to the database can slow down the working of the server. To prevent this, move the database to a separate machine.

Ensure that the server and database computers are connected by a fast network connection, and that their clocks are synchronized.

You can move the TLMA database (using backup and restore commands) only to a computer which has the same operating system installed. For example, moving the database from a computer with Windows to a computer with Linux installed is not supported.

1. Stop the Tivoli Asset Discovery for Distributed server.
2. Use DB2 to create a backup of the TLMA database.
3. Run installer and install the database component on the target computer. Installer creates an empty database which needs to be replaced.
4. On the new computer, restore the backup of the database that you created on the previous computer.
5. On the original computer, uninstall the database component and drop the database.
6. Change the configuration of the server data source to enable the server to connect to the database in its new location. The same procedure applies to both the embedded and stand-alone WebSphere Application Servers.

   To learn how to configure the connection with DB2, see:Configuring the connection between the server and the database.

Configuration settings

This section provides information about the configuration settings for the Tivoli Asset Discovery for Distributed server and how you can modify some of them to tune Tivoli Asset Discovery for Distributed to suit your needs.

The timing of events, in particular of services on the administration server is determined by two factors: the start time and the period between events. Each event has a parameter that determines its frequency. The start time is determined by the time that the server last started. The only exception of this rule is the **aggregationUsageTime** parameter described in *Tivoli Asset Discovery for Distributed server settings in the system.properties file*.

Configuration files

Configuration files define the Tivoli Asset Discovery for Distributed server and agent settings. The parameters in the configuration files are supplied with default values on installation. You may want to look at the description of each of the parameters and determine whether the value should be changed to provide enhanced performance or more readily-available information.

Most parameters fall within a specific range of values. If you specify a value that is outside the range, the default value for the setting is used.

You can edit the following configuration files:

- log.properties
- system.properties.

You can find the files in the following location:

- on the embedded WebSphere Application Server: *TAD4D install dir*\eWAS\systemApps\isclite.ear\tad4d_admin.war\WEB-INF\conf
- on the stand-alone WebSphere Application Server: *TAD4D install dir*\IBM\WebSphere\AppServer\systemApps\isclite.ear\tad4d_admin.war\WEB-INF\conf

Other configuration files should not be edited except under direct instruction from IBM Software Support personnel.

For any changes to a configuration file to take effect, stop and restart the appropriate server after changing the file.

The log.properties file

The `log.properties` file defines the trace parameters for the Asset Discovery for Distributed server.

The trace parameters (**itlm.tracelogger.level**, **itlm.tracefilehandler.maxFileBytes**, **itlm.messagefilehandler.maxFiles**, **itlm.tracefilehandler.maxFiles** and **itlm.messagefilehandler.maxFileBytes**) are the only parameters in the `log.properties` file that can be changed and reloaded while the server is running. See the "Troubleshooting and support" section of the information center for full details. After you have modified the settings, use the logreload command to reload them.

There are two `log.properties` files, located in the following directories:

- on embedded WebSphere Application Server:

- <*INSTALL_DIR*>\eWAS\systemApps\isclite.ear\tad4d_admin.war\WEB-INF\conf
- <*INSTALL_DIR*>\eWAS\profiles\AppSrv01\installedApps\cell1\LMT-TAD4D_Agent_message_handler.ear\com.ibm.license.mgmt.msghandler.web.war\WEB-INF\conf.

• on stand-alone WebSphere Application Server:
- <*WAS_INSTALL_DIR*>\IBM\WebSphere\AppServer\systemApps\isclite.ear\tad4d_admin.war\WEB-INF\conf
- <*WAS_INSTALL_DIR*>\IBM\WebSphere\AppServer\profiles\AppSrv01\installedApps\cell1\LMT-TAD4D_Agent_message_handler.ear\com.ibm.license.mgmt.msghandler.web.war\WEB-INF\conf.

The system.properties file

The system.properties file is the main configuration file for the server. You can edit the settings in this file to change the configuration of the server and agents, and the notification settings.

If the server is installed on the bundled version of WebSphere Application Server included in the Asset Discovery for Distributed installation package, the system.properties file is located in the directory <*INSTALL_DIR*>/eWAS/systemApps/isclite.ear/tad4d_admin.war/WEB-INF/conf. If you installed Asset Discovery for Distributed on a standalone application server, the file is in the directory <*INSTALL_DIR*>/WebSphere/AppServer/systemApps/isclite.ear/tad4d_admin.war/WEB-INF/conf

Server settings

Table 49. Server parameters in the system.properties file

Parameter	Units	Default	Minimum	Maximum
	Description			
productInventoryBuilderPeriod	minutes	300	300	4320 (3 days)
	The interval of time between consecutive builds of the inventory on the server. At this interval of time, the server reconciles the installed software information collected by the agent, which identifies the software components that are installed on monitored computers, with the product information held on the server. In this way the inventory of components is converted to an inventory of products, in which components are assigned according to the catalog information and the mappings of shared components.			
vmManagerPollingInterval	minutes	30	30	10080
	The interval of time between consecutive data retrievals from VM managers.			
agentVmManagerDetachmentPeriod	minutes	1440	180	10800 (7.5 days)
	The maximum idle time before an agent managed by a VM manager is considered detached. From that point in time the data sent by an agent will not be augmented by data retrieved from the VM manager.			
maxSubsequentCredentialFailures	integer	3	0	100
	The maximum number of failed attempts to log in to the VM manager. After the set number of failed connection attempts, the account is locked. The value *0* indicates unlimited attempts.			

Table 49. Server parameters in the system.properties file (continued)

Parameter	Units	Default	Minimum	Maximum
	Description			
aggregateUsageTime	time	00:00		
	The daily start time for aggregations of the data in the inventory tables (in the local time). The aggregation process aggregates qualifying inventory information (see **maxAggregateUsageAge** below) by product and server, and stores it in the corresponding history tables. Each aggregation is logged in the server trace file.			
maxAggregateUsageAge	days	2	2	14
	The age of the use data (in days) before it is included in the aggregations of the unaggregated software use database tables. This setting is used to ensure that all the relevant data for an aggregation has arrived at the server, taking into account the frequency with which it is uploaded from the agent. **Important:** It is recommended that the value of this parameter is greater than the value of the upload_usage_period parameter to ensure that all the relevant use data is aggregated.			
inventoryScanGracePeriod	hours	1	1	336
	The period of time during which agents are to send inventory data back to the server. After that the software scan is marked as failed.			
inventoryScanAllowedClockSkew	Hours	1	0	6
	The amount of time that the agent can start the scan before the specified time. It is used to identify the inventory scan which had started a little before the scheduled start. If it is turned on "1", it will allow to treat the scan from, for example, Friday 5.55 p.m. as the scan from Friday 6.00 p.m. and not Thursday 6.00 p.m. (if scans are done every day).			
websiteWithPVUs	text			
	Link to an ftp server where files with PVU tables can be found: `ftp://ftp.software.ibm.com/software/tivoli_support/misc/CandO/PVUTable/`			
maxPdfRows	8000		1	16000
	The maximum number of rows that can show up on a PDF file retrieved from the UI. This number is twice the number of maximum offering instances that can show up in an audit report PDF. For example, if **maxPdfRows** is specified to be 8000, up to 4000 instances can show up in the report.			
SwKBToolURL	text			
	The URL of the SwKBTool. The URL must have the following format: `protocol_name://hostname:port/`			
reportPath	text			
	The path to the directory where the report will be generated prior to signing. If there is not enough space in the default directory, the signing will fail.			

Agent settings

Table 50. Agent parameters in the system.properties file

Parameter	Units	Default	Minimum	Maximum
	Description			
maxAgentInactivity	minutes	10080 (1 week)	1440 (1 day)	129600 (3 months)
	The maximum time that an agent does not communicate before it is considered inactive.			
maxAgentInactivityToDelete	minutes	43200 (30 days)	20160 (2 weeks)	129600 (3 months)
	The maximum time after which an agent which is considered inactive will be removed from the system.			
discoveryMinConfidenceLevel	integer	90	0	100
	Describes the minimum confidence level for imported discovery results to be saved in the database.			

E-mail configuration settings

On the Tivoli Asset Discovery for Distributed server, notifications relate to license events and are generated in response to changes in server or agent status, and the completion of inventory scans. For more information about notifications, see the information on event logging and notifications in the "Troubleshooting and support" section of the Tivoli Asset Discovery for Distributed infocenter.

Table 51. E-mail configuration parameters in the system.properties file

Parameter	Units	Default	Minimum	Maximum
	Description			
smtpServer	text			
	The host name or IP address of a valid SMTP server. This server is used to forward the e-mail communications generated by the notification component of the server. The text must include only US ASCII characters.			
mailSender	text			
	The e-mail address that is to be used by the server as the sender address when notifications are generated. The text must include only US ASCII characters.			

```
#Mail Settings
smtpServer=mailserv.pl.ibm.com
mailSender=lmt@slmdomain.com
```

Configuration settings stored in the Tivoli Asset Discovery for Distributed server database

The Tivoli Asset Discovery for Distributed server database stores configuration settings for the Tivoli Asset Discovery for Distributed server and agents.

Tivoli Asset Discovery for Distributed server settings

This table shows the Tivoli Asset Discovery for Distributed server parameters defined in the server database.

To set the value of a server configuration parameter, enter the following command into the Tivoli Asset Discovery for Distributed command-line interface:

```
setserverconf -k <parameterName> -v <parameterValue>
```

Table 52. Administration server parameters in the configuration database.

Parameter	Units / Description	Default	Minimum	Maximum
testEnvironmentEnabled	Boolean	false	false	true
	Enables the change of the environment into test mode.			
agentToServerSecurityLevel	integer	0	0	2
	Determines the level of security to be used for communications between agents and the msghandler server. Possible values are: **0** Communication is through the unsecure port. **1** Communication is through the secure port with server authentication. **2** Communication is through the secure port with server and client authentication. **Note:** Agents with medium security levels can communicate with msghandler server that has security levels of minimum (0) or medium (1), provided that both the secure and unsecure ports are configured. If the maximum security level is used, both the agent and its msghandler server must be aligned with the security level set to maximum.			
fipsEnabled	Boolean	false	false	true
	Determines whether FIPS 140-2 certificated modules are to be used to transmit encrypted data. Possible values are: **false** Encrypted data is transmitted using default modules. **true** Encrypted information is transmitted using FIPS 140-2 certificated modules.			
storeUser	Boolean	true	false	true
	This is used to implement the privacy policy. The permitted values are: **true** Information regarding the identification of the user is recorded with the use data. **false** No information regarding the identification of the user is recorded with the use data.			
catalogBuilderPeriod	minutes	1440 (1 day)	60	10080 (1 week)
	The period of time between consecutive builds of the catalog.			
nodeTag	text	`%VENDOR %TYPE %NAME`		
	The structure to be used when the Asset Discovery for Distributed server assigns node tags during automatic creation of node records.			
divisionPluginLevel	integer	1	0	2
	Defines how the agent will plug in to the default scan group. The possible settings are: **0** The agent will never plug in to the default scan group. **1** The server will try to plug the agent in to the scan group that has been defined for it. If the group does not exist, the server will plugin the agent to the default group. **2** The agent will always plug in to the default scan group; the server ignores the scan group the agent has sent even if it exists.			

Table 52. Administration server parameters in the configuration database. (continued)

Parameter	Units	Default	Minimum	Maximum
	Description			
showAgentStatus	Boolean	true	false	true
	Shows agent status.			

Agent settings

This table shows the parameters defined in the server database.

Note: The agent parameters that you can manage using the agent configuration management feature include the parameters that control the scheduling of software and hardware inventory scans. The principal means of the scheduling software scanning is by using the Web UI task. You can change the scan-related parameters using the agent configuration management commands, but for consistency with the scan scheduling methods you cannot make changes at individual agent level.

Use the `setagentconf` command to change the value of a parameter. For a detailed description of the syntax of this command, see the setagentconf command in the "Commands" section of the information center.

Table 53. Agent configuration parameters

Parameter	Units	Default	Minimum	Maximum
	Description			
native_scan_enabled	Boolean	disabled	no	yes
	Enables scanning native registry during software scan so that the agents start uploading information to the server about unmatched registry software.			
inv_start_date	date	The date of inclusion in the database		
	The date and time when the first or only occurrence of the software inventory scan is performed. The format is `YYYY-MM-DD.hh.mm`.			
hw_inv_start_date				
	The date and time when the first or only occurrence of the hardware inventory scan is performed. The format is `YYYY-MM-DD.hh.mm`.			
inv_rate_type	integer	3	0	3
	Defines the unit in which the **inv_rate_value** parameter is expressed. The **inv_rate_type** together with **inv_rate_value** define the repetition period of the software scan. Possible values are: **0** No repetition. **1** 1 day **2** 7 days (a week) **3** 30 days (a month) For example, if **inv_rate_type=3** and **inv_rate_value=5**, the software scan will repeat every five months.			

Table 53. Agent configuration parameters (continued)

Parameter	Units	Default	Minimum	Maximum
	Description			
hw_inv_rate_type	integer	3	0	3
	Defines the unit in which the **hw_inv_rate_value** parameter is expressed. The **hw_inv_rate_type** together with **hw_inv_rate_value** define the repetition period of the hardware scan. Possible values are: **0** No repetition. **1** 1 day **2** 7 days (a week) **3** 30 days (a month) For example, if **inv_rate_type=3** and **inv_rate_value=5**, the hardware scan will repeat every five months.			
inv_rate_value	integer	1	1	9999
	The number of repeating periods, as defined by **inv_rate_type**, that separate consecutive occurrences of the software scan.			
hw_inv_rate_value	integer	1	1	9999
	The number of repeating periods, as defined by **hw_inv_rate_type**, that separate consecutive occurrences of the hardware scan.			
update_enabled	integer	0	0	2
	Indicates the status of the agent self-update service. Possible values are: **0** Disabled. **1** Periodic: agents check for new versions at regular periods defined by the **update_period** parameter. **2** Scheduled: agents check for new versions during a period of time defined by the start date specified by the **update_start** parameter and the length of the update period defined by the **update_interval** parameter.			
update_period	minutes	10080 (1 week)	1440 (1 day)	129600 (3 months)
	The interval between checks for the presence of a new version of the agent on the server when **update_enabled** is set to *1*.			
update_start	date	The date of inclusion in the database		
	The date and time and time at which the agent scheduled self-update time window starts if the **update_enabled** parameter is set to *2*. Self-update is available from this date and time for the number of hours specified for the **update_interval** parameter. The format is `YYYY-MM-DD-hh.mm`			
update_interval	hours	6	1	24
	The length of time for which the agent scheduled self-update remains open if the **update_enabled** parameter is set to *2*. Self-update is available from the date and time specified by the **update_start** parameter.			
ping_period	minutes	60	60	360
	The length of time the agent waits between checks of the connection to the server when the connection is not available.			

Table 53. Agent configuration parameters (continued)

Parameter	Units	Default	Minimum	Maximum
	Description			
down_parms_period	minutes	360	180	10080 (1 week)
	The interval between downloads of the agent parameters from the server. In addition to the parameters, at each download the agent checks the date of the last catalog update at the server, and also downloads the catalog if its own catalog is older.			
upload_usage_period	minutes	180	180	10080 (1 week)
	The interval between uploads of any data to the server. **Important:** It is recommended that the value of this parameter is smaller than the value of the max_aggregate_usage_age parameter to ensure that all the relevant data is aggregated.			
proc_list_period	seconds	300	60	600
	The frequency with which the agent checks the list of running processes for applications' use monitoring.			
was_check_period	minutes	1440 (1 day)	120 (2 hours)	2880 (2 days)
	The interval at which the agent checks to ensure that the WebSphere Application Server agent is running and updates theWebSphere Application Server discovery results. If an agent does not discover a WebSphere Application Server instance it will multiply the value of this parameter by 6.			
remote_scan_enabled	Boolean	yes	no	yes
	It determines if an agent has to scan remote file systems. If the value is *no*, the agent detects the disks but it does not scan them.			
sys_update_period	minutes	30	30	10080 (1 week)
	Defines the frequency of scanning processor.			
hw_scan_enabled	Boolean	1	0	
	0 Disabled **1** Enabled			

Agent configuration

This section describes the means to manage changes in agent configuration using a set of commands to be issued from the Tivoli Asset Discovery for Distributed command line.

It provides the following capabilities:

- To set agent parameters at all agents level or scan group level.

  A parameter inherits a value from a different parameter unless it is specified in other way. For example, if you set a value for a parameter at scan group level, all agents in that scan group will use that value unless a different value has been set for agents.

  If you want the new value that you have applied at a higher level to apply to lower levels that have their own values set, you can choose to remove or suspend the values that are set at the lower levels. Values that have been suspended can later be reinstated.
- To schedule agent self-update to be performed in a specified timeslot.

- To suspend or activate defined values for agent parameters at all agents level or scan group level.

  The state of the defined parameter can be set to active or hold. By controlling the state of parameters you can prepare an agent configuration ahead of time, putting each parameter on hold until the time comes to activate the new configuration.
- To view details of the parameter values applied at all agents level or scan group level.

Configuration changes that you make using the commands are stored in the Tivoli Asset Discovery for Distributed server database and are then downloaded to agents. Take into account the time required for download services between the Tivoli Asset Discovery for Distributed server and agents when defining configuration changes, in particular date settings that are in the immediate future.

Summary of agent configuration commands

This topic contains a list of the commands introduced for the agent configuration management feature.

Table 54. Agent configuration commands

Command	Description
setagentconf	Sets the value and, optionally, the state of the agents configuration parameter.
getagentconf	Retrieves the values of configuration parameters for a specific agent.
delagentconf	Deletes the value of a configuration parameter for a specified agent.

Enabling the agent self-update

You can enable the agents to self-update using the setagentconf command on all platforms. Self-update of Asset Discovery for Distributed agents allows you to upgrade them without changing their configuration parameters. You can enable them to self-update automatically whenever a fix pack or a new version is released.

Agents self updates are based on the local time zones in which agents are located and not the time on the Asset Discovery for Distributed server. This is important if you are managing computers from distant locations, e.g. on different continents. For example, if you schedule the agents to download and install updates at midnight (in different time zones), it will result in agents contacting the sever at different times (relative to the server time).

For large environments, especially ones approaching the maximum number of agents for one server, performance problems may occur while the agents are being updated. To avoid that, you can schedule the update for different scan groups at different times. See the setagentconf command in the Commands section of the information center.

To schedule the agents to self-update:

1. Start the Asset Discovery for Distributed command line interface.
2. To enable the agents' self-update enter the setagentconf command: `-d scanGroup | -all -k update_enabled -v value -s active`, where:

-d scanGroup
The name of the scan group for which the configuration is being set (i.e. configuration will be set for the whole scan group rather than particular agents).

-all Sets the configuration key for all agents.

You might also want to enable self-update only for a specific scan group (This is an example only).

-k update_enabled
Required. Specifies the name of the agent configuration parameter.

-v value
Specifies if the self-update facility is enabled. Possible values are:

- 0 - disabled
- 1 - enabled periodic update with the specified start date and frequency
- 2 - enabled update scheduled in a temporary time frame

-s active
Specifies the state of the configuration parameter. When it is set to active, the value of the parameter is used.

Note: During the self-update from Tivoli License Compliance Manager 2.3, Fix Pack 4 and 5 on Windows, the wdlssp command fails and the self-update ends with no action. To avoid this problem:

a. Stop the agent with the tlmagent **-e** command.
b. Open **Start** → **Control Panel** → **Administrative Tools** → **Services** → **Tivoli License Mgr Agent**.
c. Go to the Logon tab.
d. Uncheck the Allow service to interact with desktop option and click OK.
e. Start the agent with the tlmagent **-g** command.

During the next download of agent parameters, each agent checks the server for a changed version of the agent deployment package for its operating system. The interval between checks is defined by the **update_period** parameter. When a new version of the package is found, the agent downloads it and applies the changes. The changes can relate to the agent itself or to one of its corequisites. If the upgrade fails to apply a change, all changes made up to that point are rolled back to leave the agent in its original state.

When all agents have been upgraded disable the self-update by setting the **update_enabled** parameter to `0` .

Scheduling the agent self-update service

Agent parameters **update_start** and **update_interval** allow you to define a time window during which the agent self-update can be performed.

Agents are able to identify the time window that has been set for updates and contact the Tivoli Asset Discovery for Distributed during that period. To find out more about agent self-update, see the *Agent self-update* topic in the information center.

Like the other agent parameters, the agent self-update settings can be applied at agent level. This provides more flexibility, allowing you to plan a staged upgrade of a group of agents and to ensure that the update processing takes place at a time that is convenient to you.

The following scenario demonstrates how to schedule the update of agents in the Sales scan group to take place between 22:00 on 10th July 2009 and 6.00 on the 11th July 2009.

1. Issue the following command to enable self-update for agents in the *Sales* scan group.

   ```
   setagentconf -d Sales -k update_enabled -v 2 -s active
   ```

2. Issue the following command to start the update period at 22:00 on 10th July 2009.

   ```
   setagentconf -d Sales -k update_start -v 2009-07-10-22.00 -s active
   ```

3. Issue the following command to end the update period at 6.00 on the 11th July 2009, by setting the update period to 8 hours.

   ```
   setagentconf -d Sales -k update_interval -v 8 -s active
   ```

Configuring a periodic agent self-update

When the periodic update option is enabled, agents check the administration server for updates at regular intervals defined by the **update_period** parameter.

The default value for this parameter is 10080 minutes (1 week).

To configure the periodic update option for the agents in the Sales scan group, issue the following command:

```
setagentconf -d Sales -k update_enabled -v 1 -s active
```

Excluding agent directories from being scanned

Excluding some directories from scan is useful if the directories are large and contain no information important from the point of view of software inventory. By excluding them, you can speed up the scanning process.

1. Enter the `tlmagent -e` command into the system command prompt. The agent stops.
2. Add **scan_exclude_dirs=**<*directory_path*> to the `tlmagent.ini` configuration file, where <*directory_path*> is the path of the directory that you want to exclude from the scan. To exclude more than one directory, enter their paths separated by a semicolon.
3. Restart the agent.
   - On AIX platforms, enter the command `startsrc -s tlmagent`.
   - On other platforms, enter the command `tlmagent -g`.

Undoing the change of excluding agent directories from being scanned

You can undo the change of excluding some directories from being scanned on an agent.

If you want to undo the change, do the following steps:

1. Stop the agent.

2. Edit again `tlmagent.ini` and delete the scan_exclude_dirs parameter.
3. Restart the agent.

Updating the number of processors on Linux390

If the total number of processors or shared processors in your environment changes, you need to update this information for all agents influenced by this change. Otherwise, the system will display wrong information.

To update the total number of processors or shared processors perform the following steps:

1. Open the `tlmsubcapacity.cfg` configuration file. The file is located in the `/etc` directory.
2. Update the **shared_pool_capacity** and **system_active_processors** parameters and save the file. The agent will read the updated file during the next hardware scan.

Agent files

The topics in this section provide the information about the default locations for agent files.

The default location of the other agent files depends on the platform on which the agent is deployed. You can change the default agent installation location when deploying the agent.

AIX agent files

The table shows the default locations for AIX agent files.

File	Description
`/var/itlm/tlmagent.bin`	The main agent file.
`/etc/tlmagent.ini`	The agent configuration file.
`/etc/tlmlog.properties`	The configuration file for the agent logging and tracing.
`/etc/tlm_mobility.cfg`	Folder containing files for excluding virtualization layers during PVU calculation.
`/var/itlm/tlmunins.sh`	Uninstall agent script.
`/var/itlm/cache/`	Folder for agent cache files.
`/var/itlm/codeset/`	Folder containing files for conversions of characters between different code sets.
`/var/itlm/nls/`	Folder containing a subfolder for each supported language. The subfolders contain the file where agent messages are defined.
`<Tivoli_Common_Directory>/COD`	The Tivoli Common Directory subfolder for Asset Discovery for Distributed. This contains message and trace logs and problem determination scripts.
`/var/itlm/wasagent/`	Folder containing the files of the agent used to identify applications running on WebSphere Application Server.
`/var/itlm/scanner/`	Folder containing configuration files and scan output. They are used by CIT scanners.

File	Description
/var/itlm/keydb/	Folder for the SSL key database (key.kdb) and password stash file (key.sth).
/tmp/itlm	Contains temporary agent files

HP-UX agent files

The table shows the default locations for HP-UX agent files.

File	Description
/var/itlm/tlmagent.bin	The main agent file.
/etc/tlmagent.ini	The agent configuration file.
/var/itlm/tlmunins.sh	Uninstall agent script.
/var/itlm/cache/	Folder for agent cache files.
/var/itlm/codeset/	Folder containing files for conversions of characters between different code sets.
/var/itlm/nls/	Folder containing a subfolder for each supported language. The subfolders contain the file where agent messages are defined.
<*Tivoli_Common_Directory*>/COD	The Tivoli Common Directory subfolder for Asset Discovery for Distributed. This contains message and trace logs and problem determination scripts.
/var/itlm/wasagent/	Folder containing the files of the agent used to identify applications running on WebSphere Application Server.
/var/itlm/scanner/	Folder containing configuration files and scan output. They are used by Common Inventory Technology scanners.
/var/itlm/keydb/	Folder for the SSL key database (key.kdb) and password stash file (key.sth).
/etc/init.d/tlm	Auto-startup script
/tmp/itlm	Contains temporary agent files
/etc/tlmlog.properties	The configuration file for the agent logging and tracing.

Linux agent files

The table shows the default locations for Linux agent files.

File	Description
/var/itlm/tlmagent.bin	The main agent file.
/etc/tlmagent.ini	The agent configuration file.
/etc/init.d/tlm	Auto-startup script.
/etc/tlm_mobility.cfg	Configuration file for excluding virtualization layers during PVU calculation (for Linux on pSeries).

File	Description
/etc/tlmsubcapacity.cfg	Configuration file for specifying the processor brand, total number of shared processors, and the number of processors assigned to the CEC (for Linux on zSeries).
/var/itlm/tlmunins.sh	Uninstall agent script.
/var/itlm/cache/	Folder for agent cache files.
/var/itlm/codeset/	Folder containing files for conversions of characters between different code sets.
/var/itlm/nls/	Folder containing a subfolder for each supported language. The subfolders contain the file where agent messages are defined.
Tivoli_Common_Directory/COD	The Tivoli Common Directory subfolder for Tivoli Asset Discovery for Distributed. This contains message and trace logs and problem determination scripts.
/var/itlm/wasagent/	A folder containing WebSphere agent responsible for monitoring the use of WebSphere Application Server and the software deployed on this serer (J2EE applications).
/var/itlm/scanner/	Folder containing configuration files and scan output. They are used by Common Inventory Technology scanners.
/var/itlm/keydb/	Folder for the SSL key database (key.kdb) and password stash file (key.sth).
/etc/init.d/tlm	Auto-startup script
/tmp/itlm	Contains temporary agent files
/etc/tlmlog.properties	The configuration file for the agent logging and tracing.

IBM i agent files

The table shows the default locations for IBM i agent files.

File	Description
QITLMAGENT	The main agent file (in the QITLM library which is a library added in the process of installing agents and stores all binary files).
CRTAGTINI EXITINST EXITLANG EXITUNINST QITLMSTRAG QITLMMSG QITLMSAMSG QITLMJOBD WASAGTLCK QITLMDFN QITLMLANG QITLMLOD	Miscellaneous agent files (in the QITLM library which is a library added in the process of installing agents and stores all binary files).
/QIBM/UserData/QITLM/conf/tlmagent.ini	The agent configuration file.

File	Description
/QIBM/UserData/QITLM/cache/	Folder for agent cache files.
/QIBM/UserData/QITLM/keydb/	Folder for the SSL key database (key.kdb).
/QIBM/UserData/QITLM/wasagent/	Folder containing the files of the agent used to identify applications running on WebSphere Application Server.
/QIBM/UserData/QITLM/tmp/	Temporary files.
/QIBM/ProdData/QITLM/codeset/	Folder containing files for conversions of characters between different code sets.
/QIBM/ProdData/QITLM/keydb/	Folder for the SSL key database template file (key.kdb).
/QIBM/ProdData/QITLM/nls/	Folder containing a subfolder for each supported language. The subfolders contain the file where agent messages are defined.
/QIBM/ProdData/QITLM/scripts/	Folder containing scripts.
/QIBM/ProdData/QITLM/conf/tlmagent.ini	The agent configuration template file.
/QIBM/UserData/QITLM/scanner	Folder containing configuration files and scan output. They are used by Common Inventory Technology scanners.
/tmp/itlm	Contains temporary agent files
<*Tivoli_Common_Directory*>/COD	The Tivoli Common Directory subfolder for Tivoli Asset Discovery for Distributed. This contains message and trace logs and problem determination scripts.

Solaris agent files

The table shows the default locations for Solaris agent files.

File	Description
/var/itlm/tlmagent.bin	The main agent file.
/etc/tlmagent.ini	The agent configuration file.
/var/itlm/tlmunins.sh	Uninstall agent script.
/var/itlm/cache/	Folder for agent cache files.
/var/itlm/codeset/	Folder containing files for conversions of characters between different code sets.
/var/itlm/nls/	Folder containing a subfolder for each supported language. The subfolders contain the file where agent messages are defined.
<*TivoliCommonDirectory*>/COD/logs/agent/trace/trace*.log	The Tivoli Common Directory subfolder for Tivoli Asset Discovery for Distributed. This folder contains message and trace logs and problem determination scripts.
/var/itlm/keydb/	Folder for the SSL key database (key.kdb) and password stash file (key.sth).
/var/itlm/wasagent/	Folder containing the files of the agent used to identify applications running on WebSphere Application Server.
/etc/init.d/tlm	Auto-startup script.

File	Description
/tmp/itlm	Contains temporary agent files.
/etc/tlmlog.properties	The configuration file for the agent logging and tracing.

Windows agent files

On Windows platforms, the agent files are created by default in the location %WINDIR%\itlm.

File	Description
tlmagent.exe	The main agent file.
tlmagent.ini	The agent configuration file.
tlmlog.properties	The configuration file for the agent logging and tracing.
tlmunins.bat	Uninstall agent script.
/tlm_mobility.cfg	Folder containing files for excluding virtualization layers during PVU calculation.
<*TivoliCommonDirectory*>/COD/	The Tivoli Common Directory subfolder for Tivoli Asset Discovery for Distributed. This contains message and trace logs and problem determination scripts.
cache\	Folder for agent cache files.
cache\licsref.dat	The agent private database file. It is only created if the agent tracing is set to MAX.
codeset\	Folder containing files for conversions of characters between different code sets.
keydb\	Folder for the SSL key database (key.kdb) and password stash file (key.sth).
nls\	Folder containing a subfolder for each supported language. The subfolders contain the file where agent messages are defined.
scanner\	Folder containing configuration files and scan output. They are used by Common Inventory Technology scanners.
tmp\	Temporary folder used by the agent.
wasagent\	Folder containing the files of the agent used to identify applications running on WebSphere Application Server.
reboot_needed.txt	A flag file, the presence of which tells the agent that the node may need rebooting. The file remains in place until the next reboot. If, when the agent was installed, the GSKit installation was not able to complete because a preexisting version of GSKit was in use on the computer, a flag is set inside the file that tells the agent not to run. In this case, the installation of GSKit is completed after the next reboot, after which the agent will be able to start.

The tlm_mobility.cfg file

The mobility.cfg file is used to exclude the source or target partition from PVU calculations after a mobility event. It performs the same function as the Classify Relocated Partitions panel.

There are two ways of managing the exclusion after mobility has taken place:

- Inventory administrator has access to Tivoli Asset Discovery for Distributed User Interface and is also the one who knows about the mobility events and their reason or may be notified about the mobility event and its reason. Inventory administrator uses the Classify Relocated Partitions on a regular basis.
- System administrator performs the partition mobility and has access to the server but does not have access to the Asset Discovery for Distributed User Interface. He can use the `tlm_mobility.cfg` file and avoid notifying the inventory administrator to perform the exclusion.

After the mobility event occurs the agent reads the file and sends the information to the server informing it which action will be taken, i.e. if the source or target partition needs to be excluded. After this information has been successfully read, the `tlm_mobility.cfg` file is cleaned up, i.e. the row stating the reason is removed. After each mobility event, in case next exclusions have to be performed using `tlm_mobility.cfg` file, the `tlm_mobility.cfg` file needs to be edited by entering the proper information again.

All the lines starting with '#' character in `tlm_mobility.cfg` file are treated as comments and ignored.

A valid entry in the `tlm_mobility.cfg` file needs to be one of the following two possibilities:

```
maintenance: source
```

or

```
maintenance: target
```

No other value is supported. In case different words are found in place of the expected ones, the agent will ignore the file and will treat it as corrupted.

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 character set (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.
3-2-12, Roppongi, Minato-ku, Tokyo 106-8711 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 Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who 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 79758 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 information 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 www.ibm.com/legal/copytrade.shtml.

Intel, Itanium, and Pentium are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.

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

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

Java and all Java-based trademarks and logos are trademarks of Sun Microsystems, Inc. in the United States, other countries, or both.

Index

F

H

I

J

K

L

M

N

O

P

R

S

T

U

V

W

X

Printed in USA

SC23-9997-00