Tivoli®

IBM Tivoli Asset Discovery for Distributed

Version 7.2

Installation Guide

IBM®

GI11-8749-00

Tivoli® IBM Tivoli Asset Discovery for Distributed
Version 7.2

Installation Guide

IBM®

GI11-8749-00

Installation Guide

This edition applies to version 7.2 of IBM Tivoli Asset Discovery for Distributed (product number 5724-S94) and to all subsequent releases and modifications until otherwise indicated in new editions.

Contents

Chapter 1. Planning the Tivoli Asset Discovery for Distributed installation

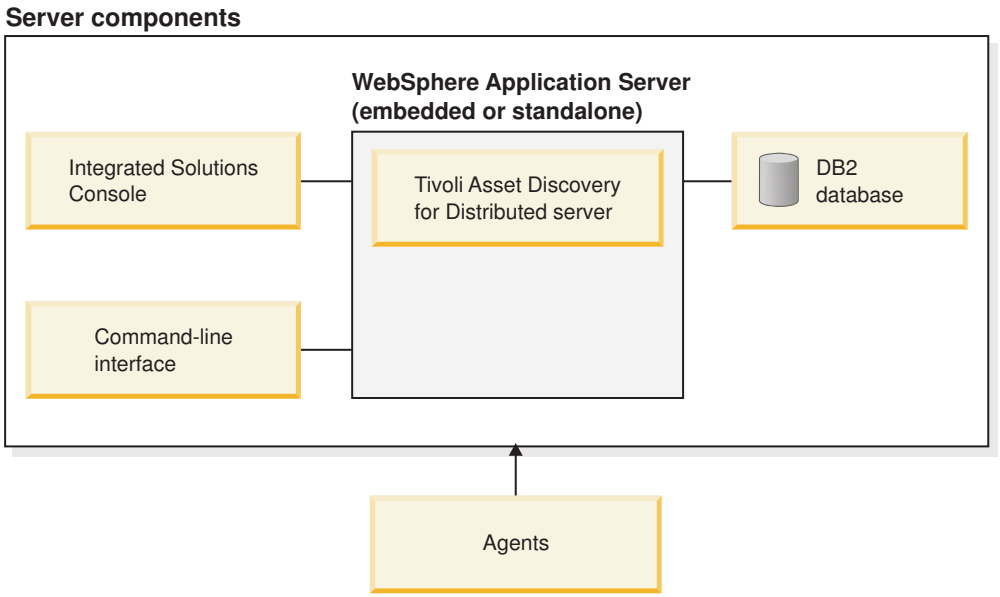
Before starting the installation, review the information in this section to learn about hardware and software requirements and other considerations.

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.

Tivoli Asset Discovery for Distributed components

Tivoli Asset Discovery for Distributed consists of a server with a DB2® database and Web interface, a command-line interface and agents installed on monitored machines.



Server components

Tivoli Asset Discovery for Distributed server
The server collects the inventory data from the agents and enables subscribed users to be notified about events which are relevant to their roles. Each installation of Asset Discovery for Distributed has a single server, which can run either on an embedded or a standalone version of the WebSphere® Application Server software.

Database
The Tivoli Asset Discovery for Distributed database stores the collected data, such as products installed on systems, processor value units (PVU) information, hardware information needed for the PVU pricing model, and configuration settings. The database runs on DB2 software.

Integrated Solutions Console
Integrated Solutions Console is the Web interface for the server. Registered users can use it to perform administrative tasks, such as producing reports of PVU capacity and inventory information over time.

Command-line interface
The command-line interface can be used to manage Asset Discovery for Distributed.

Agents
Agents are installed on each operating system that should be monitored by Tivoli Asset Discovery for Distributed. They perform hardware and software scans and forward the results to the server.

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 installing 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 server and database installation.

You can install the Tivoli Asset Discovery for Distributed server and database on the same computer, or on two different machines. When installing the database, you can also select whether you want to install the DB2 database software, which the Tivoli Asset Discovery for Distributed database runs on, or whether it is already installed on your system. 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 to install the Tivoli Asset Discovery for Distributed server on a standalone application server (recommended for large environments with more than 5000 agents), visit WebSphere Application Server information center for space requirements: http://publib.boulder.ibm.com/infocenter/wasinfo/v7r0/index.jsp?topic=/com.ibm.websphere.nd.doc/info/welcome_nd.html.

Important: In addition to the space requirements described below, remember to reserve some space for the database in the database location. When you sign a report, it is at first generated and stored as an XML file on your hard disk 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 installation only.

Operating system	Installed components	Directory	Required space
AIX	Server and database, including the DB2 prerequisite	Product installation directory	1941 MB
		DB2 installation directory	507 MB
		Database installation directory	562 MB
		/tmp	632 MB
		/etc	under 1 MB
		/var	under 1 MB
	Server and database without the DB2 prerequisite	Product installation directory	1941 MB
		Database installation directory	553 MB
		/tmp	632 MB
		/etc	under 1 MB
		/var	259 MB
	Server only	Product installation directory	1941 MB
		/tmp	632 MB
		/etc	under 1 MB
		/var	under 1 MB
	Database, including the DB2 prerequisite	Product installation directory	125 MB
		DB2 installation directory	507 MB
		Database installation directory	562 MB
		/tmp	632 MB
		/etc	under 1 MB
		/var	125 MB
	Database without the DB2 prerequisite	Product installation directory	125 MB
		Database installation directory	553 MB
		/tmp	121 MB
		/etc	under 1 MB
		/var	125 MB

Operating system	Installed components	Directory	Required space
HP-UX	Server and database, including the DB2 prerequisite	Product installation directory	1873 MB
		DB2 installation directory	1537 MB
		Database installation directory	2973 MB
		/tmp	349 MB
		/etc	under 1 MB
		/var/tmp	418 MB
	Server and database without the DB2 prerequisite	Product installation directory	1873 MB
		Database installation directory	517 MB
		/tmp	343 MB
		/etc	under 1 MB
		/var	under 1 MB
		/var/tmp	418 MB
	Server only	Product installation directory	1845 MB
		/tmp	343 MB
		/etc	under 1 MB
		/var/tmp	418 MB
	Database, including the DB2 prerequisite	Product installation directory	293 MB
		DB2 installation directory	1537 MB
		Database installation directory	2973 MB
		/tmp	349 MB
		/etc	under 1 MB
		/var	under 1 MB
		/var/tmp	418 MB
	Database without the DB2 prerequisite	Product installation directory	293 MB
		Database installation directory	472 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	Server and database, including the DB2 prerequisite	Product installation directory	1889 MB
		DB2 installation directory	830 MB
		Database installation directory	556 MB
		/tmp	121 MB
		/etc	under 1 MB
		/var	under 1 MB
		/var/tmp	under 1 MB
	Server and database without the DB2 prerequisite	Product installation directory	1889 MB
		Database installation directory	509 MB
		/tmp	591 MB
		/etc	under 1 MB
		/var	under 1 MB
		/var/tmp	under 1 MB
	Server only	Product installation directory	1889 MB
		/tmp	591 MB
		/etc	under 1 MB
		/var	4 MB
		/var/tmp	under 1 MB
	Database, including the DB2 prerequisite	Product installation directory	296 MB
		DB2 installation directory	830 MB
		Database installation directory	556 MB
		/tmp	121 MB
		/etc	under 1 MB
		/var	2 MB
		/var/tmp	under 1 MB
	Database without the DB2 prerequisite	Product installation directory	296 MB
		Database installation directory	509 MB
		/tmp	121 MB
		/etc	under 1 MB
		/var	2 MB

Operating system	Installed components	Directory	Required space
Solaris	Server and database, including the DB2 prerequisite	Product installation directory	1999 MB
		DB2 installation directory	1262 MB
		Database installation directory	2370 MB
		/tmp	216 MB
		/etc	under 1 MB
		/var	260 MB
		/var/tmp	259 MB
	Server and database without the DB2 prerequisite	Product installation directory	1999 MB
		Database installation directory	472 MB
		/tmp	182 MB
		/etc	under 1 MB
		/var	222 MB
		/var/tmp	222 MB
	Server only	Product installation directory	1971 MB
		/tmp	182 MB
		/var	259 MB
		/var/tmp	259 MB
	Database, including the DB2 prerequisite	Product installation directory	181 MB
		DB2 installation directory	1262 MB
		Database installation directory	2370 MB
		/tmp	216 MB
		/etc	under 1 MB
		/var	259 MB
		/var/tmp	260 MB
	Database without the DB2 prerequisite	Product installation directory	181 MB
		Database installation directory	508 MB
		/tmp	181 MB
		/etc	under 1 MB
		/var	under 1 MB

Operating system	Installed components	Directory	Required space
Windows	Server and database, including the DB2 prerequisite	Product installation directory	1662 MB
		DB2 installation directory	530 MB
		/tmp	590 MB
		Database installation directory	437 MB
	Server and database without the DB2 prerequisite	Product installation directory	1881 MB
		DB2 installation directory	under 1 MB
		/tmp	590 MB
		Database installation directory	437 MB
	Server only	Product installation directory	1881 MB
		/tmp	590 MB
	Database, including the DB2 prerequisite	Product installation directory	123 MB
		DB2 installation directory	530 MB
		/tmp	590 MB
		Database installation directory	437 MB
	Database without the DB2 prerequisite	Product installation directory	123 MB
		DB2 installation directory	under 1 MB
		/tmp	112 MB
		Database installation directory	437 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
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

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

Version	Required level, service packs, patches
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 10 for EM64T and AMD64	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 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
9 for Intel x86	Service Pack 3, compat-libstdc++ The following 32-bit version packages: pam cracklib-dicts cracklib glib2 libselinux

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

Version	Required level, service packs, patches
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 three options for installing the DB2 software prerequisite:

- You can choose to install it at the same time as Asset Discovery for Distributed, from the installation wizard.
- You can install 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 versions of WebSphere Application Server

For large production environments, you may want to install the server on a base version of WebSphere Application Server, instead of the embedded version that can be installed as a part of Asset Discovery for Distributed.

Asset Discovery for Distributed supports the following version of WebSphere:

- WebSphere Application Server, version 6.1, Fix Pack 23
- WebSphere Application Server Network Deployment, version 6.1, Fix Pack 23 (standard application server profile only).

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 9. 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 10. 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)	

Table 10. Supported versions of IBM i (formerly known as i5/OS) (continued)

Version	Levels, service packs, patches, compatibility packs	Partitioning technologies
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 11. 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 12. 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

Table 12. Supported versions of Red Hat Enterprise Linux (continued)

Version	Levels, service packs, patches, compatibility packs	Partitioning technologies
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	
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

Table 12. Supported versions of Red Hat Enterprise Linux (continued)

Version	Levels, service packs, patches, compatibility packs	Partitioning technologies
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 13. 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
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 14. 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
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

Table 14. Supported versions of SUSE Linux Enterprise Server (continued)

Version	Levels, service packs, patches, compatibility packs	Partitioning technologies
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 15. 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 16. 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 17. 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 18. 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
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

Table 18. Supported versions of Windows (continued)

Version	Levels, service packs, patches, compatibility packs	Partitioning technologies
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	
Windows 2000 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 Advanced Server		

Table 18. Supported versions of Windows (continued)

Version	Levels, service packs, patches, compatibility packs	Partitioning technologies
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 19. 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 20. Tivoli Asset Discovery for Distributed agent space requirements

Operating system	Directory	Space required

Table 20. Tivoli Asset Discovery for Distributed agent space requirements (continued)

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.
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.

Table 20. Tivoli Asset Discovery for Distributed agent space requirements (continued)

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.
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.

Table 20. Tivoli Asset Discovery for Distributed agent space requirements (continued)

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.
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.

Table 20. Tivoli Asset Discovery for Distributed agent space requirements (continued)

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.
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.

Table 20. Tivoli Asset Discovery for Distributed agent space requirements (continued)

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.
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
	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 21. 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.

Installation considerations

There are different installation types of the Tivoli Asset Discovery for Distributed that you might choose from, depending on your business needs.

You can choose one of the three scenarios for Asset Discovery for Distributed installation:

Proof-of-concept installation
This type of installation allows you to check if the elements of the infrastructure can communicate with one another efficiently. The database parameters are scaled down to allow fast communication between product components and quick testing. After performing proof of concept installation, you can run the production installation of Asset Discovery for Distributed.

Installing the server and database on one computer
This is the recommended installation type but it should only be used if the computer on which you are installing the product meets the "CPU and memory requirements for the server and database" on page 2.

Installing the server and database on different computers
In this scenario, the server and database components are installed on two different computers. You can decide to use it if the computer on which you want to install does not meet the hardware requirements, or if you have an existing instance of DB2 installed. In the first case, you will need to run the installation program twice: once to install the database on the machine where the DB2 should run, and the second time to install the administration server on the computer designated for it. If you have DB2 already installed on a different computer than the one where you want to install the server, you will need to locate the existing instance of the database during the server installation. The installation will create the Asset Discovery for Distributed database in the existing DB2 and populate it with data, such as the pre-defined software catalog and the PVU table. It will also create the `tlmsrv` database user used to connect to the database, in case it does not already exist.

Proof-of-concept installation

You can perform a proof-of-concept installation of the server before the actual production installation. Proof-of-concept installation allows you to quickly set up an environment, check if it is working and if it satisfies your business needs.

Proof-of-concept installation has all the functionality of the production version, but the database parameters are scaled down and the communication times between product components reduced. This mode of installation, does not allow you to install the Administration server and Administration server database on separate computers. You can launch a proof-of-concept installation by selecting **Test Environment** at the start of the server installation.

Note: Proof-of-concept installation can be performed only on the embedded version of WebSphere Application Server. After you finish testing, you can later install the server in production mode either with the embedded application server or on a base version of WebSphere Application Server.

Below you will find a comparison of parameter values between test (Proof of Concept) and production environment installations.

Table 22. Proof Of Concept and production installations

System.properties		**Test environment**	**Production environment**
Server	**productInventoryBuilderPeriod** (minutes)	60	300
	maxAggregateUsageAge (days)	1	2
	inventoryScanGracePeriod (hours)	1	10
Agent	**maxAgentInactivity** (minutes)	30	10080
	maxAgentInactivityToDelete (minutes)	43200	43200
Db configuration			
Server	**BUFFERPOOL**	20000	80000
	testEnvironmentEnabled	true	false
Agent	**down_parms_period** (minutes)	7	360
	upload_usage_period (minutes)	5	360
	ping_period (minutes)	2	60

After you have tested the configuration by performing the proof-of-concept installation, you can begin installing the Tivoli Asset Discovery for Distributed server and agents.

IBM Tivoli Asset Discovery for Distributed 7.2 Hardware Sizing

This document provides a summary for planning and recommendations based on the results from the Tivoli Asset Discovery for Distributed 7.2 performance tests.

Configuration of the test environment

The focus in the document is on the consumption of resources during the agent login, Inventory Builder and Aggregation processes. The hardware recommendations are based on achieving reasonable execution time to reconcile the installed software information collected by the agent.

In a Tivoli Asset Discovery for Distributed installation with thousands of agents, the largest consumer of CPU resource and time are the inventory builder and aggregation processes.

The Linux on System z test environment was a z990-2084 LPAR configured with 2 dedicated processors. The environment was running with 1.49 GB of RAM, which is less than the recommended minimum (2 GB), and this has a large impact on the elapsed time to complete longer running tasks such as inventory building.

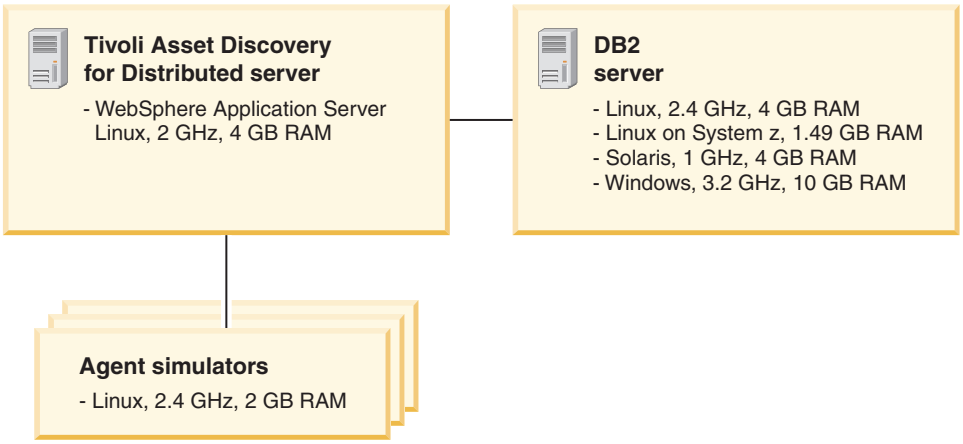


Figure 1. The configuration of test servers

Tivoli Asset Discovery for Distributed hardware recommendations

Hardware recommendations for Tivoli Asset Discovery for Distributed 7.2 environments with up to 50000 agents, and 50 products per agent.

Table 23. Hardware recommendations for Tivoli Asset Discovery for Distributed 7.2 environments

Requirements for	Type	Topology	Processor	RAM	Hard drive disk
Tivoli Asset Discovery for Distributed server (without DB2)	Minimum	two computers	2.4 GHz (Uniprocessor)	2 GB	30 GB
Tivoli Asset Discovery for Distributed server (without DB2)	Recommended	two computers	2.4 GHz (2-way)	3 GB	30 GB
DB2 server	Minimum	two computers	2.4 GHz (2-way)	2 GB	30 GB
DB2 server	Recommended	two computers	3.4 GHz (2-way)	6 GB	40 GB
Tivoli Asset Discovery for Distributed server (with DB2)	Minimum	one computer	2.4 GHz (2-way)	4 GB	40 GB
Tivoli Asset Discovery for Distributed server (with DB2)	Recommended	one computer	3.4 GHz (2-way)	6 GB	40 GB

For any large scale database management system updates, it should be ensured that statistics are collected as soon as possible. The simplest method to collect statistics is to invoke the following DB2 command: reorgchk update statistics on table all.

Recommended machines for the above configurations can include:

- IBM System XSERIES 335
- IBM System XSERIES 336
- IBM System XSERIES 3650

The general disk configuration requirements are:

- WebSphere Application Server: 50 GB
- DB2 server: 150 GB

It is recommended that a dedicated network interface be provided between the WebSphere Application Server and the database server. The general recommendation is at least a 100 MB/s connection between the two servers.

Capacity planning

Table 24. Suggested hardware requirements for two-server configurations

Number of Agents	Product component	1-10 products	11-35 products	36-50 products
Fewer than 5000 agents	WebSphere Application Server	1 core, 2 GB	1 core, 2 GB	1 core, 2 GB
	DB2	1 core, 2 GB	1 core, 2 GB	2 core, 3 GB
5000 - 50000 agents	WebSphere Application Server	2 cores, 2 GB	2 cores, 2 GB	2 cores, 4 GB
	DB2	2 cores, 3 GB	2 cores, 3 GB	2 cores, 4 GB
50000 - 100000 agents	WebSphere Application Server	2 cores, 3 GB	2 cores, 4 GB	2 cores, 4 GB
	DB2	2 cores, 3 GB	2 cores, 6 GB 64-bit operating system is recommended for DB2 server.	2 cores, 6 GB 64-bit operating system is recommended for DB2 server.

Tuning recommendations

The following properties are recommended:

Table 25. WebSphere Application Server parameters

Parameter	Values
Java Virtual Machine Heap	initial heap size: 256, maximum heap size: 1024
Default Thread Pool	maximum size: 100
Message Handler Thread Pool	maximum: 50
Web Container Thread Pool	maximum size: 250
LMT Connection pools	maximum connections: 10
LMTHW Connection pools	maximum connections: 10
Connection pools for Message Handler Data Source	maximum connections: 101 (2 times threads +1), for more than 25000 agents with 50 products installed

Table 26. DB2 parameters

Parameter	Values
Logfilesize	5000 (for more than 25000 agents, 50 products)
Logprimary	120

Table 26. DB2 parameters (continued)

Parameter	Values
Logsecond	80

Increasing the size of the transaction log for greater than 25000 agents at 50 products per agent prevents the transaction log from being filled. If the transaction log is full – aggregation will not run. Trace logs will contain:

```
<Exception><![CDATA[com.ibm.db2.jcc.b.SqlException: The
transaction log for the database is full.
```

Increase maximum connections for the MsgHandler data source especially for greater than 25000 agents at 50 products per agent to avoid reaching maximum connection limits. If maximum connections are reached then these messages may occur in SystemOut.log.

```
;------Start of DE processing------ =
[10/18/09 16:56:04:482 EDT] , key = com.ibm.websphere.ce.j2c.ConnectionWaitTimeoutException Max
connections reached
```

Note: It may also be possible to avoid maximum connection by increasing the **timeout** period.

Single-server versus separate servers installations

Installing Tivoli Asset Discovery for Distributed and DB2 on separate computers will be beneficial for aggregation if CPU resource is constrained.

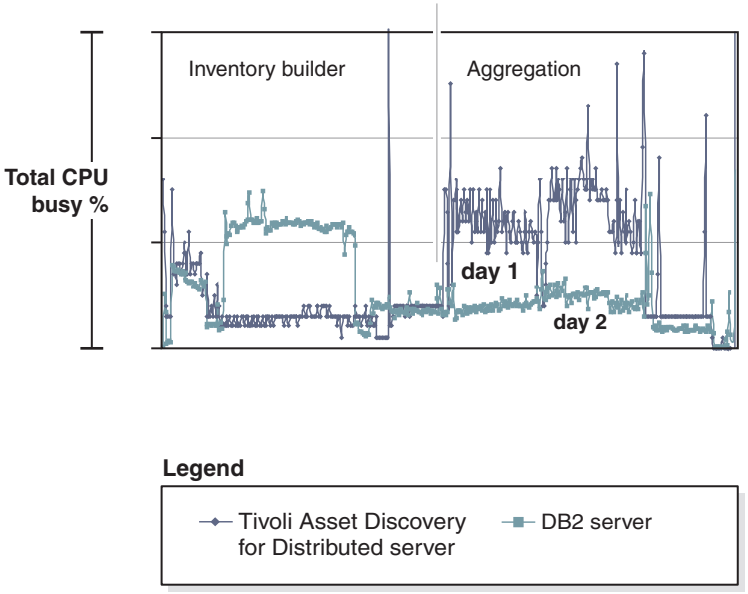


Figure 2. Diagram showing the CPU activity of the two separate test servers

The top usage of CPU resource and time in Tivoli Asset Discovery for Distributed 7.2 operations is the inventory builder and aggregation processes. Splitting the WebSphere and DB2 onto separate servers could be slightly beneficial during aggregation if CPU resource is already constrained. Generally when Inventory Builder is active on DB2, WebSphere Application Server is relatively inactive and vice versa.

Database size and disk usage

The ultimate size of the database depends on a number of factors such as the number of agents, products per agent, DB2 operating system, inventory builder, and aggregation processes.

Database size

You need to estimate 75000 bytes per agent for UNIX based systems and 30000 bytes per agent for Windows based systems at initial agent login. You should estimate an additional 75000 bytes per agent for UNIX based systems after inventory builder and aggregation have completed.

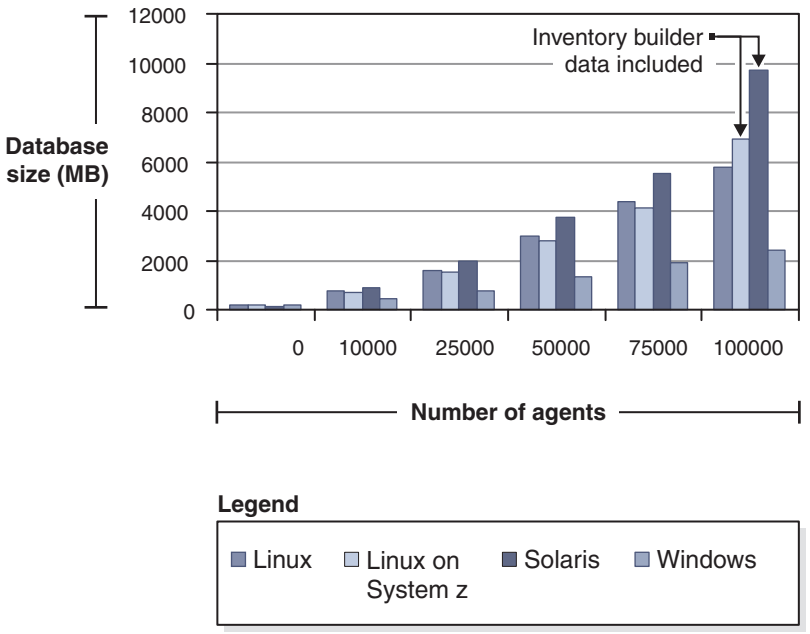


Figure 3. DB2 database size increase (in megabytes) after initial agent database population

Database size results were obtained by using the DB2 command db2 call get_dbsize_info. The **dbsize** information was obtained immediately after agents logged into the server. The database sizes listed (in megabytes) generally do not include additional table growth which will result from inventory builder and aggregation processes.

The following table lists increased database size for Linux on System z and Solaris DB2 servers after the inventory builder process completed.

Table 27. Increased database size for Linux on System z and Solaris DB2 servers, in megabytes

Agents	Linux	Linux on System z	Solaris	Windows
0	186	195	145	196
10000	747	721	864	420
25000	1582	1510	1939	767
50000	2988	2824	3741	1317
75000	4393	4138	5538	1877
100000	5802	**6892** (inventory builder included)	**9738** (inventory builder included)	2438

The following is a simple rule for calculating the database space:

- Estimate 75000 bytes per agent for UNIX based systems and 30000 bytes per agent for Windows based systems at initial agent login.
- Estimate an additional 75000 bytes per agent for UNIX based systems after Inventory Builder and Aggregation have completed.

The tests used 50 products per agent. The number of products per agent will affect the database size result.

The database size for Windows after inventory builder and aggregation have completed is not measured here, but we can assume based on the UNIX results that an additional 30000 bytes per agent would be consumed.

Results of tests with the use of datagen workload

Tests have confirmed that the greatest database and disk usage growth occurs on initial agent login and also during inventory builder process.

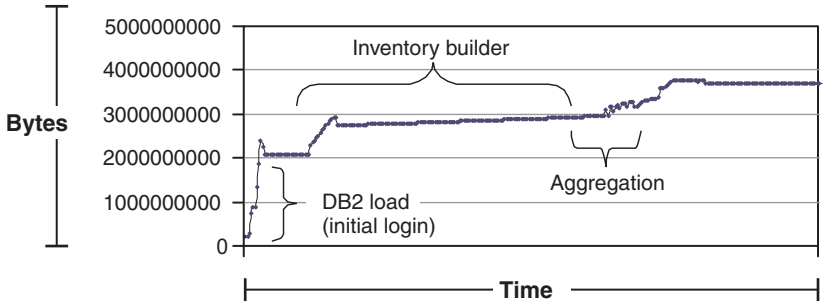


Figure 4. Database size increase on Linux on System z for initial agent login, inventory builder and aggregation

Table 28. Database size increase in megabytes

Database delta	Megabytes
load.sql	1875.378
Inventory builder	1197.761
Aggregation	470.614

The size of the database in the test with 50000 agents consumed 1.9 GB on initial agent login, an additional 1.2 GB after inventory builder process completed and another 470 MB after aggregation completed. The disk usage delta's track with the database size increases.

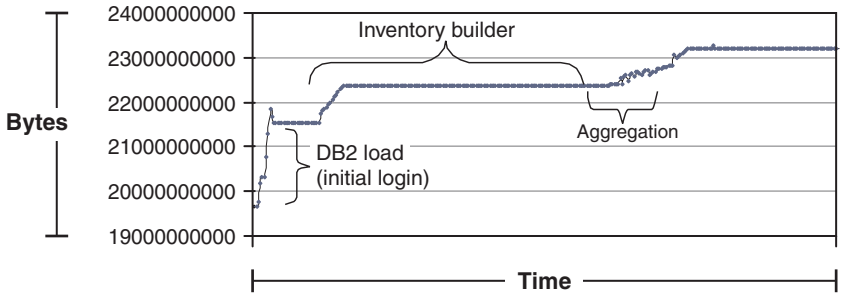


Figure 5. Disk usage increase on Linux on System z for initial agent login, inventory builder and aggregation

Table 29. Disk delta increase in megabytes

Disk delta	Megabytes
load.sql	1881.666
Inventory builder	1185.116
Aggregation	462.2746

Results of tests with the use of agent simulator workload

In the test with 50000 simulated agents, inventory builder contributes to the database growth the most, with aggregation and agent simulator login causing comparable database size growth. Disk usage delta is similar to the database size increase.

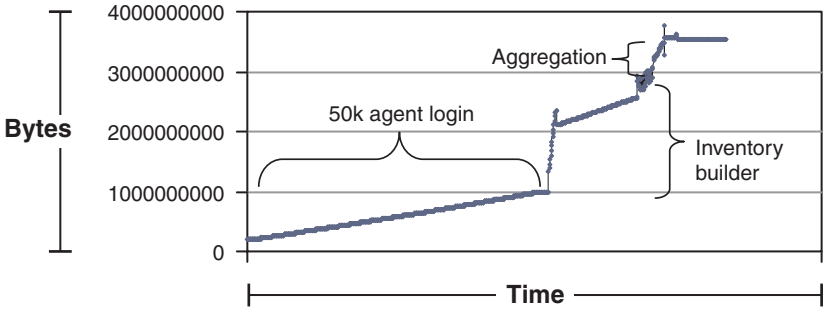


Figure 6. Database size increase on Linux on System z for initial agent simulator login, inventory builder and aggregation

Table 30. Database size increase in megabytes

Database delta	Megabytes
Agent simulator login	793.3
Inventory builder	1886.1
Aggregation	598.3

The size of the database in the test with 50000 simulated agents consumed 800 MB on initial agent login, an additional 1.9 GB after inventory builder process completed and another 600 MB after aggregation.

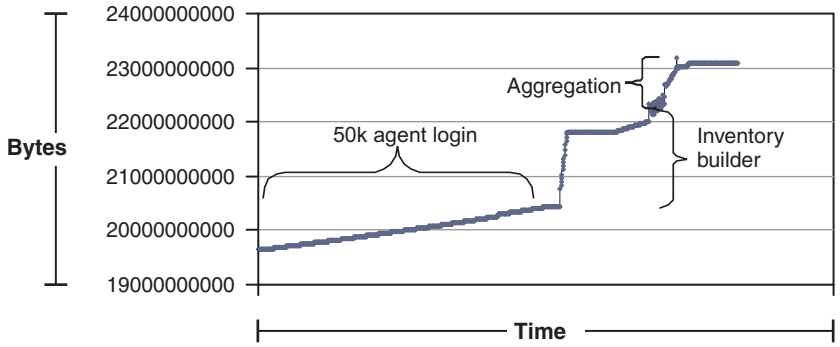


Figure 7. The increase of disk usage on Linux on System z for initial agent simulator login, inventory builder and aggregation

Table 31. Disk delta increase in megabytes

Disk delta	Megabytes
Agent simulator login	777.0
Inventory builder	1 915.9
Aggregation	571.3

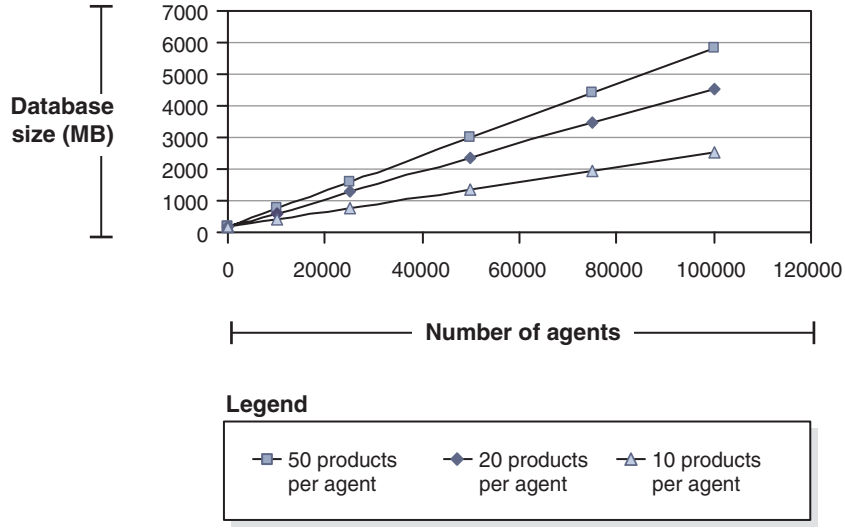


Figure 8. Database size growth depends on the number of products per agent

The diagram shows that with the number of agents rising the database grows most rapidly when there are up to 10 products installed on a computer. The growth then slows down even though the number of products installed on a computer is substantially higher, for example 50.

Table 32. Database size results when the number of products per agent is varied from 10 to 50

Number of agents	Linux - 10 products	Linux - 20 products	Linux - 50 products
0	177	177	186
10000	410	614	747
25000	757	1269	1582

Table 32. Database size results when the number of products per agent is varied from 10 to 50 (continued)

Number of agents	Linux - 10 products	Linux - 20 products	Linux - 50 products
50000	1338	2361	2988
75000	1919	3453	4393
100000	2503	4545	5802

The results are for initial agent login only, additional increases will occur after inventory builder and aggregation have completed.

Inventory builder process time versus DB2 RAM size

Reducing the amount of RAM increases the amount of time it takes to complete the inventory builder process. For most configurations, a minimum of 3 GB of RAM should be sufficient for satisfactory completion times of inventory builder.

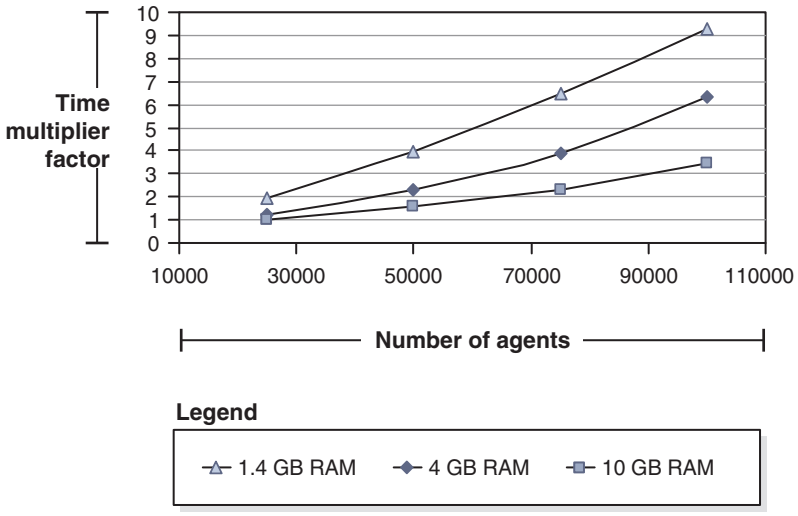


Figure 9. Time projections for the inventory builder process

The time used by the inventory builder process for 25000 agents with 50 products per agent on a system with 10 GB of RAM is normalized to a value of 1. The same 10 GB (DB2) machine would take 3.5 times as long to run the inventory builder process if 100000 agents were used. A 4 GB computer would take 6.5 times as long to run the process with 100000 agents installed.

Tools and data generation scripts

Datagen population tool is used to populate DB2 database with agent information. Agent simulator uses separate machines to simulate agents that also send inventory and usage data to the Tivoli Asset Discovery for Distributed server.

Parameters

The datagen population tool resides on the DB2 server. It can be used to vary the number of agents and products per agent and mix of PVU and non PVU as well as the number of days for aggregation. The tool generates an .sql file and then loads the database using the db2 –tvf load.sql command.

Shell script to track database size over time for Linux on System z

```
#!/bin/sh
echo ------------------------------------------------
db2 connect to tlma
rm -rf size.out
MOST_EPS=1000
LEAST_EPS=0
INCREASER=1
echo ------------------------------------------------
while [ $LEAST_EPS -lt $MOST_EPS ]
do
db2 "call get_dbsize_info(?,?,?,0)" | grep "Value :" > temp
head -2 temp > temp.1
tail -1 temp.1 >> size.out
date >> size.out
LEAST_EPS=`expr $LEAST_EPS + $INCREASER`
sleep 60
done
```

Linux commands that track inventory builder and aggregation in logs and check for log exceptions

```
ls -alrt /usr/ibm/tivoli/common/COD/logs/admin/trace/
cat /usr/ibm/tivoli/common/COD/logs/admin/trace/* | grep -i "Inventory Builder Task -
STARTED TIME"
cat /usr/ibm/tivoli/common/COD/logs/admin/trace/* | grep -i "AGGREGATION - STARTED
TIME"
cat /usr/ibm/tivoli/common/COD/logs/admin/trace/* | grep -i "SQLException: The
transaction log"
cat /opt/IBM/WebSphere/AppServer/profiles/AppSrv01/logs/server1/SystemOut.log | grep
-i "ConnectionWaitTimeoutException"
```

Chapter 2. Installing and setting up Tivoli Asset Discovery for Distributed

Tivoli Asset Discovery for Distributed is a separately installable component of Tivoli Asset Management for IT. This component generates reports about installed licenses, which software asset managers use for monitoring compliance. After you have planned your Asset Discovery for Distributed infrastructure, you are ready to start installing the product.

An overview of the installation process

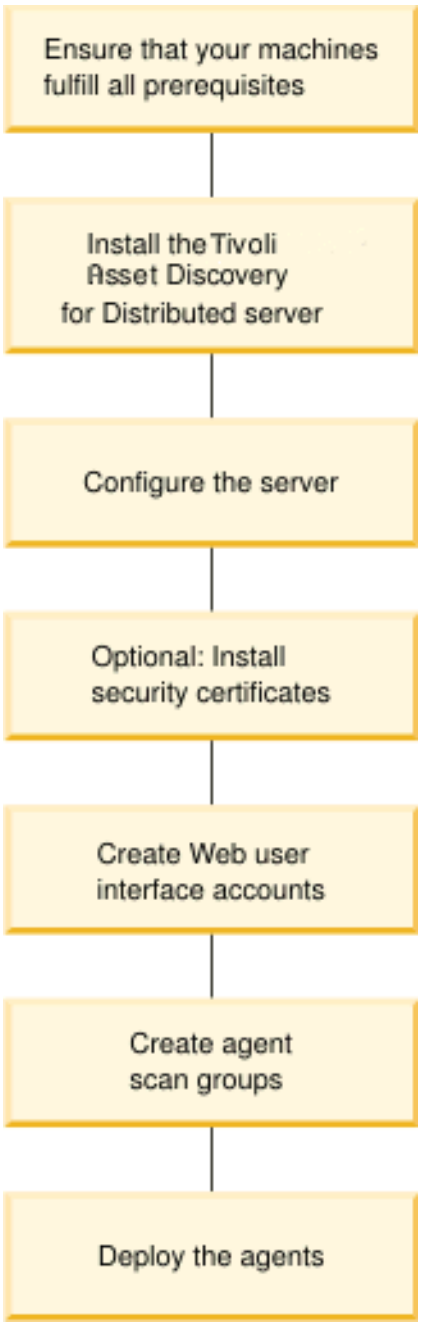
Before Tivoli Asset Discovery for Distributed is ready for use, you need to install and configure the server and its database, then deploy the agents.

Before you begin

Plan your installation.

- Ensure that your server and agent machines fulfill all hardware and software prerequisites.
- Plan the topology.
- Consider whether you want to use secure communications for the server and agents.

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



To do this:

1. Install the server and database. You might also need to install the prerequisites.
2. Configure the server. This includes both required and optional tasks, as follows:

   Required

   - Import the IBM catalog to populate the database with information about products that can be monitored.
   - Import the processor value unit table to have up-to-date information about your processor value unit capacity.

   Optional

- Configure proxy servers for communications between the server and agents.
- Configure the server to send e-mail notifications about significant licensing and system management events.
- Configure the process of discovering nodes where agents have to be installed.
- Add users.

3. If you have decided to use secure communications:
   a. Install certificates for the server and prepare certificates for the agents. Refer to the "Security" section of the information center for more information.
   b. Create accounts for the users who will work on the Web user interface. For more information, see Controlling access in the "Security" section of the information center.
4. Install agents on the systems that you want to monitor.

Software packages for installing Tivoli Asset Discovery for Distributed 7.2

To perform the installation, 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 install 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 33. Installation packages for installing on the embedded and stand-alone WebSphere Application Server

No	Type of image	If you install on embedded WebSphere Application Server	If you install 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 installation.
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 33. Installation packages for installing on the embedded and stand-alone WebSphere Application Server (continued)

No	Type of image	If you install on embedded WebSphere Application Server	If you install 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 installing 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	

Installing the server

Start the Tivoli Asset Discovery for Distributed installation by installing the server and database.

Before you begin

Ensure that the machine where you are installing the server fulfills all hardware and software requirements.

If you have downloaded the installation image from Passport Advantage®, ensure that you have prepared the files for installation.

Important: If you are installing DB2 in language version other than English, it is recommended that you install DB2 before the server component.

To do this:

1. If you want to install the database on a separate machine, ensure that the clocks of server and database computers are synchronized.
2. UNIX Linux Install and activate the Korn shell.
3. Red Hat Set SELinux to permissive or disabled.
4. Install the application server and database. Depending on the size of your working environment, you can choose one of the following options:
   - Install together with the version of WebSphere Application Server that is embedded with the product. This method is recommended for small to medium environments (up to 5000 agents).
   - Install on a full, base version of WebSphere Application Server. This method is recommended for large environments (up to 45000 agents). This alternative is highly configurable and requires advanced administrative skills. You can install the base edition of WebSphere Application Server that is bundled with Asset Discovery for Distributed or you can use a working installation of the application server. In both cases it is recommended to create a dedicated profile on the application server to effectively separate Asset Discovery for Distributed from other applications running on it.
5. Reboot the system and start the Web user interface to verify the server installation.

Preparing files for installation

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

Synchronizing the clocks of server and database computers

If you have decided to install the server and the database on separate computers, the time difference between the two computers should not be grater than 300 seconds. A greater time difference might result in data loss or corruption in the server database.

If the clocks are not synchronized, the server will start in problem determination mode, and some features will not be accessible.

Use a non-manual method of clock synchronization, for example Network Time Protocol. All recent UNIX and Windows systems have the ability to synchronize with Network Time Protocol servers. For other operating systems, refer to user documentation for information how to configure time synchronization.

The following example shows how you can ensure that the clocks are synchronized the Windows XP operating system. The method shown here requires that both computers are connected to the Internet.

1. On the application server, open the Windows Control Panel and select **Date and Time**.
2. On the **Internet Time** tab, select the time of the server that you want to synchronize with.
3. Repeat this operation on the computer where you will install the database.

Changing SELinux settings before installing Tivoli Asset Discovery for Distributed on Red Hat Linux

Red Hat enterprise Linux enables SELinux by default, which is incompatible with Tivoli Asset Discovery for Distributed. To ensure proper server installation, you need to change the SELinux setting from enforcing mode to either permissive or disabled.

This change must be permanent because turning enforcing mode back on prevents the server from working.

Beware of inadvertently preserving `enforcing` mode by changing the context to `textrel_shlib_t` for all the libraries used by server.

1. Open the `/etc/selinux/config` file.

2. Change the **SELINUX** parameter to `permissive` or `disabled`.
3. Restart the computer.

Installing Tivoli Asset Discovery for Distributed with the embedded version of WebSphere Application Server

For small to medium-sized environments (up to 5000 agents), you can select to automatically install the version of IBM WebSphere Application Server that is embedded in the Tivoli Asset Discovery for Distributed installation images. Both products are installed into the same target directory.

Installing the server in interactive mode

Use the installation wizard to specify all parameters as the installation proceeds.

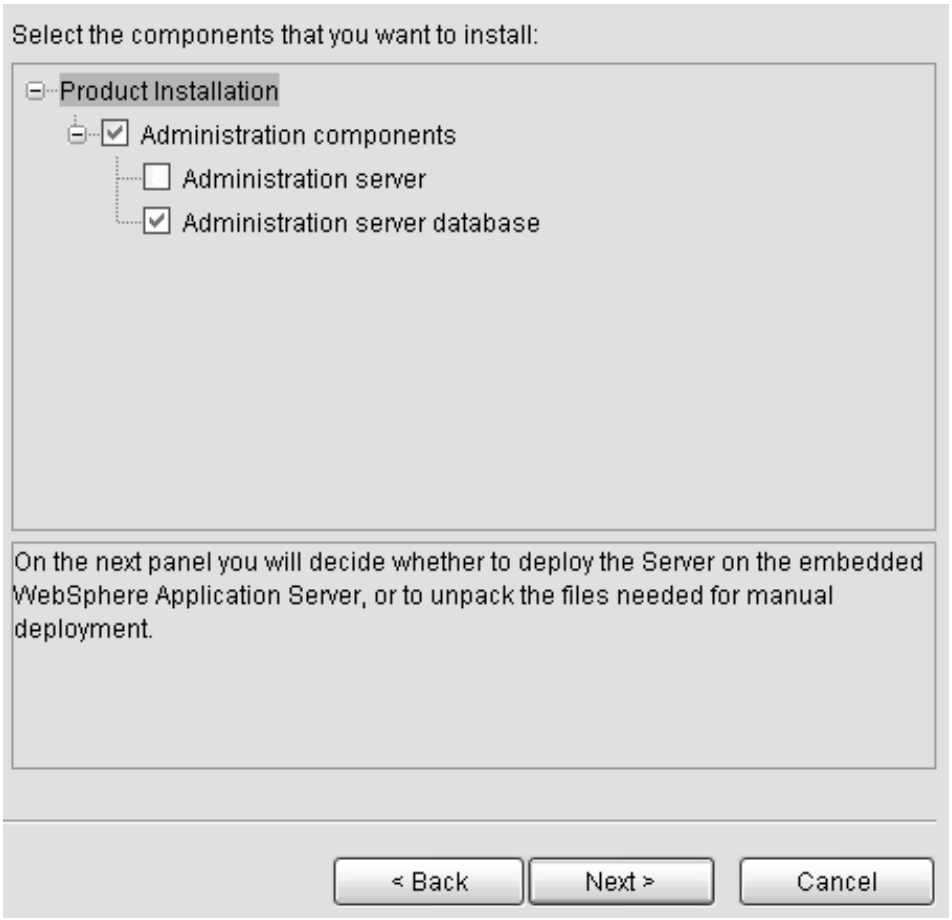
Before you begin

On UNIX and Linux machines, there must be graphical interface available. Otherwise, you must use silent mode.

If you have downloaded the installation image from Passport Advantage, ensure that you have prepared your files for installation.

1. In the directory where you unpacked the installation files, run **launchpad.exe** (Windows) or **launchpad.sh** (other platforms). The Welcome page opens. You can also launch the installation file `TAD4D-server-7.2-`*`your_platform`*`.bat` (Windows) or `TAD4D-server-7.2-`*`your_platform`*`.sh` (other platforms) directly from the `DIRECTORY_WITH_INSTALLATION_FILES\server`. You do not need the Web browser for this method. You are directed straight to the language selection window.
2. In the left-hand navigation bar, 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. After accepting the terms of the license agreement, specify the type of installation that you want:
   - For a typical installation, select **Production Environment**.
   - For a proof of concept, select **Test Environment**.
6. Specify the installation location.

   Note: If you are installing on Solaris, do not select a location in the tmpfs file system. A known problem prevents the calculation of available space in this file system.
7. Select the components that you want to install. You can install the server and database on the same computer or on different computers. If you have already installed a component on this computer, or you are running the proof-of-concept installation, that selection is unavailable.

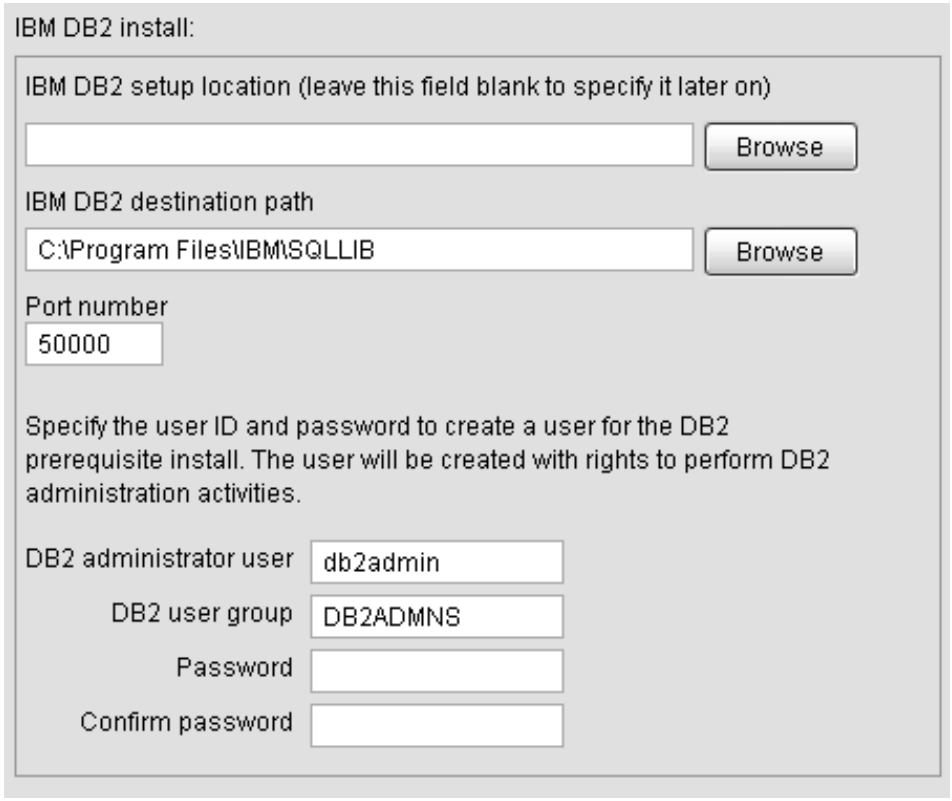


If you have decided to install the database on a different computer than the server, you need to run the installer twice on each of the computers. It is recommended to start with the database installation. This way you will be able to test the connection between the server and the database and after completing the installation on both computers, the server will not need to be restarted to work.

8. Click **Next** to begin the installation.
9. If you are installing the database on this computer, specify whether to install the IBM DB2 software that is bundled with this program, or whether to use an existing instance of DB2 on this computer. Click **Next**.

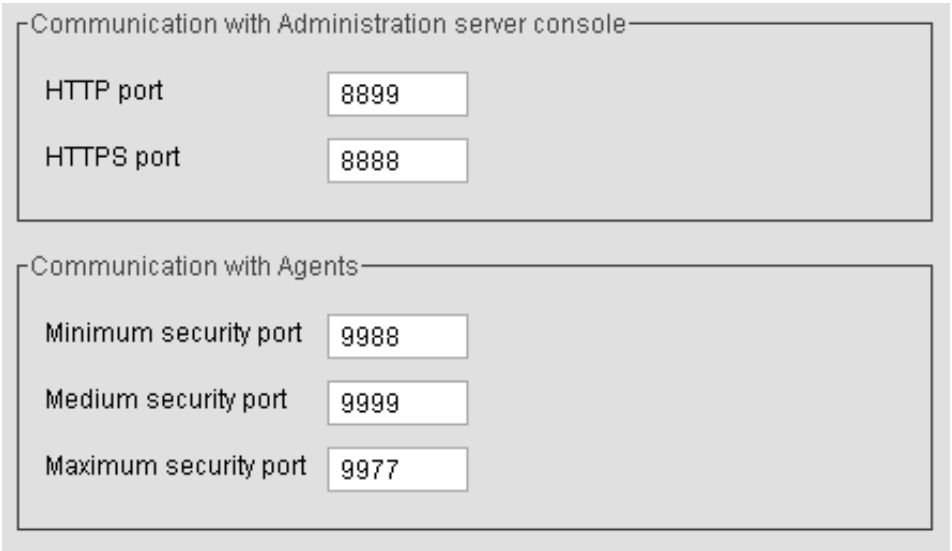
   Note: UNIX A known problem causes the installation wizard to consider the last element on the DB2 instance owner file path (with home directory in it) the DB2 instance owner name, thus if your DB2 instance owner home directory does not follow the pattern `<unix_home_dir>/<db2_instance_owner_name>`, create 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 of database component.
10. If you are installing the bundled version of DB2 on this computer, specify the following configuration settings:
    - **IBM DB2 setup location**. You can leave this field empty and specify it later.
    - **IBM DB2 destination path** - the directory where you want to install the DB2 software.
    - **Port number** - the number of port to use when communicating with the administration server.

- **User ID and password**.



Note: Do not install DB2 using the Asset Discovery for Distributed installer if DB2 is already installed on the target machine.

11. Click **Next**. Accept or change the ports for communication with the server console and agents. The installer checks if the ports you selected are already in use, and lets you know if there are any conflicts.



12. Specify the password for the `tlmsrv` user ID, which is responsible for authorized DB connection and is used by server processes to access the

database. The password must adhere to the security requirements of the server. Depending on your operating system, there might be different rules, such as minimum length.

The `tlmsrv` is stored in encrypted form in the application server configuration files.

13. If you chose to install the database on this computer, use the **Specify security settings** check box to specify whether to use secure communications between the server and agents.
14. If you selected to use secure communications, define the security settings:

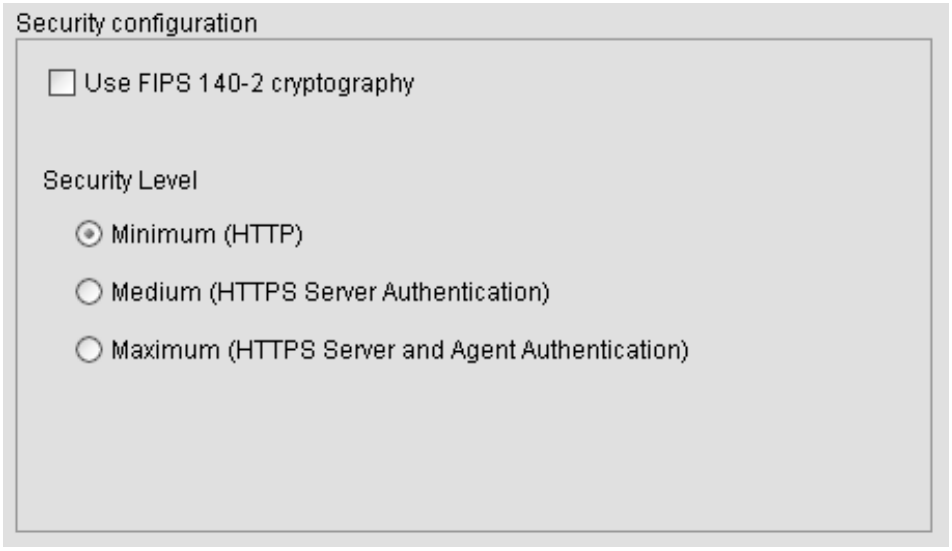
Use FIPS 140-2 cryptography

This option is available only when you are installing the server. Select it to enable the encryption of data using approved algorithms from the Federal Information Processing Standard 140–2. This setting applies to the server that communicates with the agents. i5/OS FIPS cannot be used on i5/OS platforms. If your environment includes even one agent running on i5/OS, FIPS cannot be turned on.

Security Level

This option is only available only when you are installing the database.

- 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 that you defined when you deploy the agent.
- If you set the maximum security level, you must set the same level of security for all agents when you deploy them.



15. Click **Next** and review the installation information.

Important: The installation program creates some temporary files, so at times more disk space is required than the total size shown on this page. Consider this extra requirement before proceeding with the installation; if necessary, clear additional space.

16. Click **Next**. The first stage of the installation commences. *Do not interrupt* this stage. If it fails for any reason, you might need to clean up files manually.

17. If you selected to install DB2 version 9.1, the Locate the Installation Image panel opens. Navigate to the DB2 installation image delivered with Asset Discovery for Distributed, select the appropriate setup file for your platform and click **Open**. This panel does not appear if you have already provided the path to the installation image in step 10. The installation of DB2 starts.
18. If you want to stop the installation at the end of the current task, click **Stop**. You can resume it later at the same point.
19. When the installation completes, click **Finish** to exit the wizard.

If you are installing the server and database on separate computers, log on to the other computer and run the installer again.

After both the server and database are installed, configure the server security, add users in the Web interface, and install the agents.

Installing the Tivoli Asset Discovery for Distributed server in silent mode

As an alternative to using the installation wizard, you can specify parameters in a response file and start the installation from a command line. Use this approach for unattended installation.

Before you begin

Linux UNIX Ensure that the `setupServers.bin` and `TAD4D-server-7.2-`*`your_platform`*`.sh` files have execution rights.

If you have downloaded the installation image from Passport Advantage, ensure that you have prepared the files for installation.

To do this:

1. Read the license agreement in the `license.txt` file. The file is located in the directory `<DIRECTORY_WITH_INSTALLATION_FILES>/license/`*`your_language`*.
2. In the `<DIRECTORY_WITH_INSTALLATION_FILES>/server` directory, edit the response file that fits your scenario:
   - For production installations, edit `installResponseProduction.txt`
   - For test installations, edit `installResponsePOC.txt`

   Important:
   a. Ensure that the **licenseAccepted** parameter is set to **true**. If you do not accept the license, the installation will fail.
   b. Do not install DB2 using the Asset Discovery for Distributed installer if DB2 is already installed on the target server.
3. To start the installation, run the following command:
   - Linux UNIX `TAD4D-server-7.2-`*`your_platform`*`.sh –options` *`response_file_path`* `–silent`
   - Windows `TAD4D-server-7.2-`*`your_platform`*`.bat –options` *`response_file_path`* `–silent`

   Where *response_file_path* is either the full or relative path to the response file you are using.

If you are installing the server and database on separate computers, log on to the other computer and run the installer again.

When both the server and database are installed, configure the server security and add users in the Web interface, then install the agents.

For more information, refer to the "Security" section of the Information Center".

Resuming a failed Asset Discovery for Distributed server installation

If the installation fails or if you stop it *after* the initial copying files to the target directory, you can resume installation after resolving the problem.

However, if the installation fails *during* the initial copy stage, you cannot resume and you might need to do manual cleanup.

This task assumes you are installing from the wizard. If you are installing from a response file, and the installation failed, resolve the problem (see the "Troubleshooting" section of this guide), uninstall the server and install it again.

Installation can be resumed by running the installation script with `-resume` switch:

- Windows `TAD4D-server-7.2-your_platform.bat -resume`
- UNIX `TAD4D-server-7.2-your_platform.sh -resume`

1. If you have not yet exited the wizard, click **Diagnose failure**. A panel opens showing the status of installation tasks.
2. To identify why the installation failed, click the task with the status `Error`. Refer to the *Troubleshooting and support* section of this guide for possible solutions.
3. If you have already exited the wizard, check the log files for information about why the installation failed. If the information in log files is not sufficient, uninstall the server and install it again.
4. When you have solved the problem, change the task status to `Ready`.
5. Click **Run All**.

Server installation response files

Response files provide input parameters that are used when you install from a command prompt or in silent mode.

There are two response files. Both are located in the directory `TAD4D-server-7.2–base/server/`. Some parameters have default values that you can accept or change. Others have no default, so you must provide a value.

Note: Some parameters are passwords and are stored in the options file in unencrypted form. Ensure that this is not against the security policy of your organization before using this installation method.

Common parameters

The following parameters are required for all installations of Tivoli Asset Discovery for Distributed, regardless of whether you are installing the server, the database or both.

Table 34. Response file parameters for all installations

Parameter	Parameter key name	Default
License agreement acceptance	**-G licenseAccepted**	true
	Delete the hash that flags this statement as a comment. The installation will fail if you do not explicitly agree with the license agreement by changing this statement from comment status.	
Installation location	**-P installLocation**	
	Specify an empty directory where the selected elements will be installed. If the directory does not exist, it will be created. If the directory path contains spaces, enclose it in double-quotation marks.	
Installation type	**-W setupType.selectedSetupTypeId**	
	Specify the type of installation to be performed. Possible values are: **Test** Installs the selected components in test (proof-of-concept) mode. Use this type of installation to quickly check if Tivoli Asset Discovery for Distributed is working and if it satisfies your business needs. **Admin** Installs the selected components in production mode. **Unpack** Unpacks the installation files needed to install the server on the base version of WebSphere Application Server. Specifying this value means that the server components will not be installed by the installation wizard. The files are unpacked into the directory specified by the **-P installLocation** parameter and you can proceed with the installation on the base WebSphere Application Server.	
Setup: administration server component selection	**-P admin.active**	true
	Specify whether or not the Tivoli Asset Discovery for Distributed server element should be installed. Possible values are: **true** The server will be installed on this computer. **false** The server will not be installed on this computer.	
Setup: administration database component selection	**-P adminDB.active**	true
	Specify whether or not the database element should be installed. Possible values are: **true** The database will be installed on this computer. **false** The database will not be installed on this computer.	
Base configuration: tlmsrv user password	**-W dbInstallAdmin.tlmsrvPwd**	
	Specify the password to be used to authenticate access to a database by server processes. This password is assigned to a user with ID tlmsrv that is created on the target computer when a database element is installed for the first time. The password is also stored in an encrypted form in a properties file on the server computer. The maximum length is 20 characters and the characters allowed are: `A-Z, a-z, 0-9, +, -, *, |, =`. The password must follow the security policy of the operating system of the computer on which it will be created. **Note:** Passwords entered in this file are not encrypted. This may be a security violation in your organization.	

Table 34. Response file parameters for all installations (continued)

Parameter	Parameter key name	Default
Base configuration: ports used by administration server	**-W baseConfig.adminPort**	8899
	The port used by the administration server console.	
	-W baseConfig.adminSSLPort	8888
	The port used by the administration server console in secure mode.	
	-W baseConfig.minSecPort	9988
	The port used for minimum security level communications.	
	-W baseConfig.medSecPort	9999
	The port used for medium security level communications (HTTPS server authentication).	
	-W baseConfig.maxSecPort	9977
	The port used for maximum security level communications (HTTPS server and agent authentication).	
Setup: Specify security parameters	**-W setSecurity.specifySecuritySettings**	false
	Specify whether or not the security parameters specified in this response file are to be used instead of default values. Possible values are: **true** Custom security parameters will be used. **false** Default security parameters will be used.	
Administration database port number	**-W dbInstallAdmin.portNumber**	
	If you are installing only the server on this machine, specify the port number to connect to the database. If you are also installing the database and the DB2 prerequisite, you can leave this field blank. The database port number is then set to the value specified for the DB2 installation in the **-W db2InputPanel.db2_port** parameter.	

Server parameters

The following parameters are only needed if you are installing the server on this computer.

Table 35. Parameters for silent installation of the Tivoli Asset Discovery for Distributed server

Parameter	Parameter key name	Default
	Description	
Administration server: remote administration database: address	**-W dbInstallAdmin.hostName**	localhost
	Supply the host name or the IP address where the administration server database will be installed. If you want to the database to be installed on the same machine as the server, set this parameter to `localhost`.	
Setup: Use FIPS 140-2 cryptography	**-W setSecurity.enableFips**	false
	Specify whether FIPS-approved encryption algorithms are to be used. Possible values are: **true** FIPS 140-2 approved cryptographic algorithms are used. **false** Default algorithms are used.	

Database parameters

The following parameters are only needed if you are installing the server on this computer. Some of them may not be required, depending on whether you are also installing the DB2 prerequisite, or whether it is already installed on your system.

Table 36. Database parameters for silent installation

Parameter	Parameter key name	Default
	Description	
Prerequisite search: IBM DB2 database server	**-W databaseServerPathPanel.prerequisiteInstalled**	false
	Specify whether a supported version of DB2 is already installed on the computer. Possible values are: **true** Indicates that the prerequisite is installed in the location specified in the **databaseServerPathPanel.locationPath** parameter key. The wizard checks that a supported version is in the specified location. If this value is selected and no version of DB2 can be found, the installation will fail. **false** Indicates that no supported version is installed. The wizard installs the bundled DB2 database server prerequisite. If any version of DB2 is already installed on the computer, the prerequisite installation will fail.	
	-W databaseServerPathPanel.locationPath	
	If a supported version of DB2 is installed (**-W databaseServerPathPanel.prerequisiteInstalled=true**), specify the location in which it is installed. It must be provided as a full pathname. If the pathname includes directories with spaces in their names, it must be enclosed in double quotes. For UNIX, supply the path of the home directory of the DB2 instance owner.	
Administration database: local instance owner (UNIX only)	**-W dbInstallAdmin.dbAdminUser**	db2inst1
	On UNIX platforms, specify the instance owner of the DB2 administration server database. If DB2 is being installed as together with the database, the instance owner is set to the value specified in **-W db2InputPanel.db2_userName** and this parameter is not used.	
DB2 prerequisite: prerequisite image location	**-W db2InputPanel.db2_setupLoc**	
	If the wizard is to install the DB2 prerequisite on a Windows server, specify the location of the setup file. It must be provided as a full pathname, and if the pathname includes directories with spaces in their names, it must be enclosed in double quotes.	
DB2 prerequisite: install location	**-W db2InputPanel.db2_instLoc**	
	If the wizard is to install the DB2 prerequisite, specify the directory in which to install it. It must be provided as a full pathname, and if the pathname includes directories with spaces in their names, it must be enclosed in double quotes. For UNIX, supply the home directory of the DB2 instance owner, that, when concatenated with the DB2 instance owner ID, gives the path to the install location of DB2. For example, if the location is `/home/db2inst1`, where `db2inst1` is the instance owner's id, enter just `/home`.	
DB2 prerequisite: DB2 port number	**-W db2InputPanel.db2_port**	50000
	If the wizard is to install the DB2 prerequisite, specify the port on which DB2 will listen.	
DB2 prerequisite: DB2 administrator ID	**-W db2InputPanel.db2_userName**	db2admin
	If the wizard is to install the DB2 prerequisite, specify the DB2 administrator user ID that the wizard will create on the computer. The ID must not exist on the computer where it is to be created, and must respect the user id rules of that computer.	
DB2 prerequisite: DB2 administrator group	**-W db2InputPanel.db2_userGroup**	
	Optional parameter. You can specify the administrator group to which the administrator ID will belong.	

Table 36. Database parameters for silent installation (continued)

Parameter	Parameter key name	Default
	Description	
DB2 prerequisite: DB2 administrator password	**-W db2InputPanel.db2_password**	
	If the wizard is to install the IBM DB2 prerequisite, specifies the DB2 administrator password that will be used when the DB2 Administrator ID is created. The maximum length is 20 characters and the characters allowed are: A-Z a-z 0-9 + - =. The password must follow the security policy of the operating system of the computer on which it will be created. **Note:** Passwords entered in this file are not encrypted. This may be a security violation in your organization.	
Agent to server security level	**-W setSecurity.agentToServerSecurityLevel**	0
	Determines the level of security to be used for communication between the agent and the server. This option is used only when installing the administration server database component. Possible values are: **0** To use unsecure communication. **1** To use secure communications with server authentication. **2** To use secure communications with client and server authentication. **Note:** 1. Agents with minimum (0) and medium (1) security levels can communicate with servers that have security levels of minimum or medium, provided that both the secure and unsecure ports are configured. If the maximum security level is used, both the agent and the server must be aligned with the security level set to maximum. 2. If you select medium (1) or maximum (2) security, you must perform a series of tasks to set up and install certificates. For full information about enabling security, see the "Security" section of the Asset Discovery for Distributed infocenter.	

Installing the Tivoli Asset Discovery for Distributed on WebSphere Application Server

As an alternative to installing the server on the embedded version of WebSphere Application Server, you can install on a full, base 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.

If you are installing on the Base version of WebSphere Application Server, with enabled secure agent-server communication, you must apply a Java update on WebSphere Application Server. You can download the update from the following page: http://www-01.ibm.com/support/docview.wss?rs=180&uid=swg24019127. If you do not apply the Java update, the secure communication will not work properly. The agent will be able to connect to the server but other operations such as catalog download will cause GSKit exceptions.

Installing WebSphere Application Server

Before you begin to install Asset Discovery for Distributed server and database, WebSphere Application Server must already be installed. If you do not already have an installed application server, you can use the installation media for the base edition of WebSphere Application Server that is bundled with Asset Discovery for Distributed.

Locate the installation media or images for WebSphere Application Server and start the setup program. For more information, consult the WebSphere documentation available in the WebSphere information center.

Configuring WebSphere Application Server

Before you begin to install Asset Discovery for Distributed server and database, WebSphere Application Server must already be present in your infrastructure. You can use a freshly-installed or working installation of WebSphere Application Server, however, it is recommended to create a dedicated profile on it to effectively separate Asset Discovery for Distributed from other applications.

For WebSphere Application Server Network Deployment, only the default (standard or base) profile is supported.

1. Create a new dedicated profile for Asset Discovery for Distributed to ensure that the product is separate from other applications installed on the WebSphere Application Server, and that it can be configured or uninstalled independently. You can use an 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 after performing any of the tasks described in this section. 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
   ```

   ```
   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.

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.

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.

Extracting the installation files from the interactive installer

Use the Asset Discovery for Distributed installation wizard to extract the files needed for installing 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. Prepare the files for installation.
2. Run **launchpad.exe** (Windows) or **launchpad.sh** (other platforms). The Welcome page opens.
3. In the left-hand navigation pane, click **Install or upgrade to Tivoli Asset Discovery for Distributed**.
4. Click **Launch the server installation wizard**.
5. Select the language of the installation and click **OK**. The installation wizard starts.
6. Click **Next**. After accepting the license agreement, click **Next** again.
7. 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.
8. Accept the default installation location or click **Browse** to select a different location. Click **Next**. This page appears only if no previous version of the application is discovered in the system.

   Note: If you are installing on Solaris, do not select a location in the tmpfs file system. A known problem prevents the calculation of available space in this file system.
9. Select **Administration server** as the component that you want to install and click **Next**.
10. 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**.
11. Specify the directory where you want to extract the files and click **Next**.
12. 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.

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 database and its prerequisites

After extracting the installation files, use the installation wizard to install the DB2 version 9.1 that is delivered with Tivoli Asset Discovery for Distributed using the installation wizard.

Before you begin

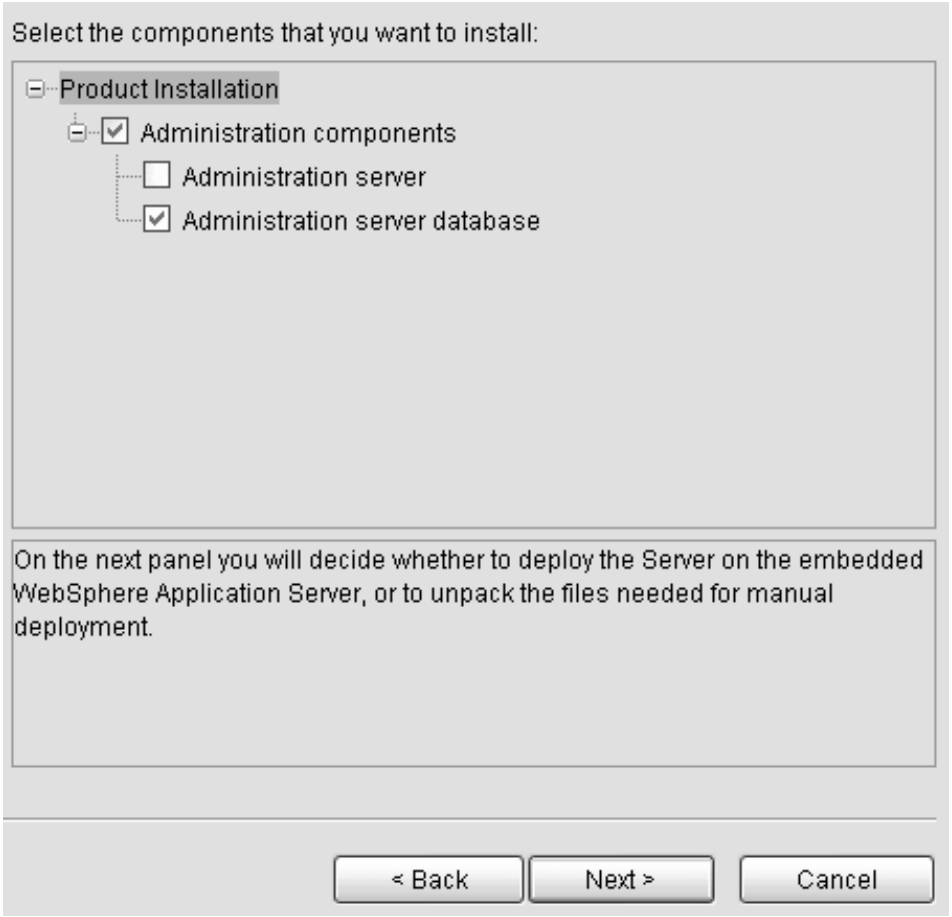
- You must have the following operating system privileges:
  - UNIX Linux root

– Windows Administrator

- The network firewall on the target computer may cause problems in communication between the database and the server. Make sure a port is available to allow for the connection with the database. The default port is 50000; you can override that at installation time.

1. Log on to the computer where you want to install the database, as a user with administrative rights (Administrator on Windows platforms or root on UNIX platforms).
2. Start the installation launchpad.
   a. When you are ready to install, click **Install or upgrade to Tivoli Asset Discovery for Distributed** and then click **Launch the server installation wizard**.
   b. After selecting your language and accepting the license agreement, click **Next**.
3. On the next page, select **Production Environment** and click **Next**.
4. Specify the installation location.

   Note: If you are installing on Solaris, do not select a location in the `tmpfs` file system. A known problem prevents the calculation of available space in this file system.
5. Click **Next**. On the next page, when prompted to select the components that you want to install, select **Administration server database**.



6. The DB2 prerequisite page is displayed. Select the option to let the wizard install DB2 and click **Next**.

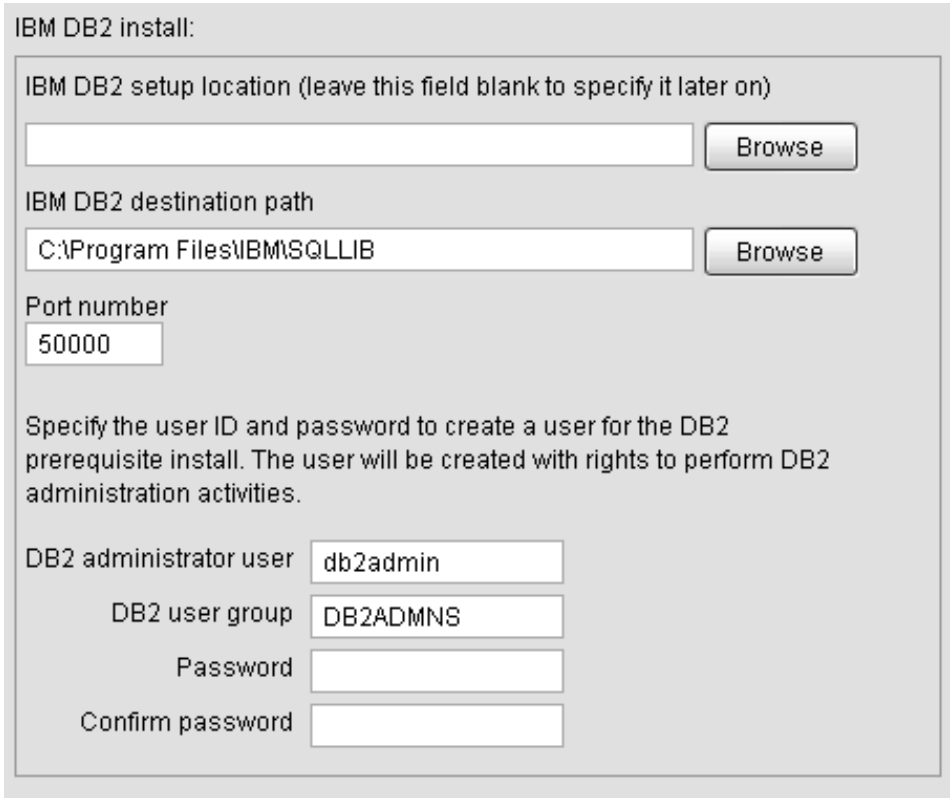
7. On the next page, supply the following information:

   IBM DB2 setup location
   (Optional) The directory where DB2 installation files are located.

   IBM DB2 destination path
   The directory where DB2 will be installed.

   Port number
   The port on which DB2 will listen.

   DB2 administrator user, DB2 user group and password
   A user ID and password pair that will be created on this computer for performing DB2 administrative tasks, such as creating and dropping databases. The User ID must not already exist on the computer, and the password must conform to any local rules that are in force. You also need to provide the name of a DB2 user group.



   Click **Next**.

8. On the next page, specify and confirm the password to be used by server processes to access the database.

   During installation of the database, the user `tlmsrv` is created with a password set to this value. The password must comply with any local rules that are in force in your environment and can contain only the following characters: `A-Z, a-z, 0-9, +, -, *, |, =` .

   Keep a note of this password. You must specify it again when you install the server. Click **Next**.

9. On the next page, define the security settings for the database server.

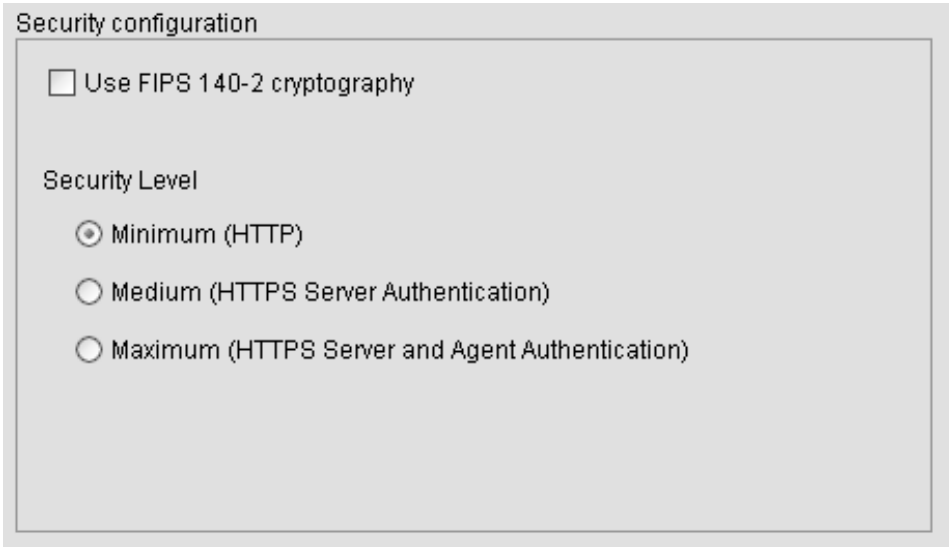
   Specify agent to server security level
   This setting has the following values:

Minimum
To use unsecure communication.

Medium
To use secure communications with server authentication.

Maximum
To use secure communications with client and server authentication.

If you set the minimum or medium security level, agents can communicate with the database 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.



A summary panel opens, showing the amount of space required for DB2 and the Tivoli Asset Discovery for Distributed server database.

10. On the installation summary page, check the information that is provided and confirm that you have enough space to complete the installation. The creation of temporary files might require more space, than the total size shown. If the amount of available space is close to the total size shown, clear some space before proceeding.
11. Click **Next** to begin the installation.

    During the first stage of the installation, files are copied. If this stage fails for any reason, you might need to clean the environment manually because the uninstaller is not created until the end of the installation process.
12. If you did not specify the location of the installation files earlier, a popup window prompts you to locate the installation image for DB2. Navigate to the installation image and select the appropriate folder in which the setup file is located for the platform where you are installing. Click **OK**.
13. The installation of the DB2 software starts, followed by set up of the database.

    Starting with the DB2 installation, the installation process is divided into a series of tasks and can be stopped at the end of a task and resumed later. A **Stop** button is available and you can click it to stop the installation at the end

of the task currently being performed. If you stop the wizard, or if the installation fails during any of these tasks, you can resume the installation from that point.

14. When the installation completes successfully, a summary panel opens showing the installation tasks that were completed. Click **Finish** to exit from the wizard.

When this procedure is successfully completed, the following results are achieved:

- Installation of the DB2 Enterprise Server Edition server, version 9.1 software that is provided with Tivoli Asset Discovery for Distributed.
- Creation of the `DB2install.log` file that traces the installation of DB2 is created. You can find it in the following location: *`Tivoli_Common_Directory`*`/COD/logs/install/trace/DB2install.log`
- Creation of the Tivoli Asset Discovery for Distributed server database
- Creation of a user ID and password pair for performing DB2 administrative tasks
- Creation of another user ID called tlmsrv and password that will be used by server processes to access the database.

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.

Installing the server components

Run the scripts extracted from the interactive installer to install the Asset Discovery for Distributed server.

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. Edit the setupWAS.properties configuration file. The file is in the `WAS-scripts` directory in the location that you specified when unpacking the files.

   Note: Parameter values are case-sensitive.

2. 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?).

3. 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.

4. 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`).
   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 37. JDBC provider properties

Parameter	Value
name	*Arbitrary name* for example *MyJDBCProvider*
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*
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 38. 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 39. 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 [$AdminConfig getid /Cell:cell_name/Node:node_name/Server:server_name/JDBCProvider:p
set ds [$AdminConfig create DataSource $provider [list [list name ds_name] [list jndiName jdbc/TL
$AdminConfig create J2EEResourcePropertySet $ds [list [list resourceProperties [list [list [list
$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 40. 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 [$AdminConfig getid /Cell:cell_name/Node:node_name/Server:server_name/JDBCProvide
set msghandler_ds [$AdminConfig createUsingTemplate DataSource $provider {{name msghandler_ds_
set pool [$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 41. TLMHW data source properties.

Parameter	Value		
name	*tlmhw_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
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 42. 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/ThreadPoolMa
$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 43. 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/Transport

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 44. Timer manager1 properties

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

Table 45. 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/TimerM
$AdminConfig create TimerManagerInfo $timerMgrProvider {{name timer_name1} {jndiName tm/LMT_Timer
```

   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 46. 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]
```

UNIX

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

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.webcon
```

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 64. 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.

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.

Installing agents - overview

After you have installed and configured the server, you can install the first agents.

Tivoli Asset Discovery for Distributed provides several methods for installing 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, deploy the agents in bulk using its software distribution functions. On Windows platforms, you can also install the agents using logon scripts.

You can install agents regardless of whether the Asset Discovery for Distributed server is running.

This topic provides an overview of the subtasks that are involved in installing agents. Some of the subtasks were covered earlier, under "Planning the installation"; others are described in the pages that follow.

Important: The agent installer does not allow you to use non-Latin characters when specifying path names (such as the agent installation path, Common Inventory Technology installation path or the temporary folder for the agent), and the scan group name. 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.

The agent response file and log file names cannot contain two-byte characters.

1. Ensure that the computer where you are installing the agent fulfills all hardware and software requirements.
2. Gather the following information:
   - Asset Discovery for Distributed server address and the port number that agents are to use.
   - Level of security that has been configured for the server.
   - The proxy port and address If you want the agent to use a proxy server for communication with the server.
3. Depending on the server security level, you might also need to create some certificates:
   - For medium or maximum security levels, you will need to prepare your own server certificate (`cert.arm`).
   - For maximum security level, you will need to prepare both your own server certificate and agent certificate (`agent_ID.kdb`).
4. UNIX If you want to install agents on a shared file system, ensure that you have exported and mounted the remote directory so as to allow changing permissions on mounted directories and files, for example chown and chmod command.
5. Configure any firewalls between the agent and server computers to allow the agent access to the server.

6. Optional: Create scan groups that you can use later for scheduling software scans, so not all agents are scanned at the same time. Scan groups are recommended for large environments. If you do not create them, all agents are added to a common, default group.

   For more information about how to create scan groups, refer to the "Administration" section of the information center.

7. 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. After running the setup file, return to execute mode by running `change user /execute`.
8. If you are installing the agent in a partitioned environment using VMware or Microsoft Virtual Server virtualization technologies, ensure that 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.
9. Red Hat Set SELinux to disabled.
10. Start the installation. Depending on your platform, you can choose one of the following actions:
    - Install the agents using the native installers for your platform. This method is available for all supported platforms.
    - Use IBM Tivoli Configuration Manager to install the agents in bulk.
    - Windows Install the agents using Windows logon scripts.
11. Set up any necessary security certificates: For medium or maximum security level, use the server certificate (`cert.arm`) during agent installation.
    - If the server is configured for maximum security level, import the agent certificate. The certificate is stored as `agent_ID.kdb` in the CMS keystore. To import the certificate, run the following command: `tlmagent -impcert agent_ID.kdb cmsPassword`. If the certificate has been delivered to *Agent_Dir*`\keydb\private` and is protected with the `slmtest` password, it will be automatically imported when the agent starts.

      i5/OS Deliver the certificate file to the i5/OS computer and use the Digital Certificate Manager (DCM) to import it.

      In the DCM Web interface, click **Manage Certificates** > **Import certificate** to import the certificate file that you transferred to the i5/OS computer to the Tivoli Asset Discovery for Distributed agent keystore database. The agent keystore is classified as **Other System Certificate Store**. You can find it under the following path: `/QIBM/UserData/QITLM/keydb/key.kdb`. Its initial password is `slmtest`. For more information about installing and using DCM, see the iSeries information center at: http://publib.boulder.ibm.com/iseries/.
12. To verify that the installation was successful, check whether 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.

Preparing agent certificates for client authentication

If you selected the maximum security level, you must perform tasks on the administration server computer to generate a set of personal certificates each of which certificate contains a unique agent ID and a public key.

1. Log on to the administration server computer as Administrator (for Windows platforms) or root (for UNIX platforms) and start the Asset Discovery for Distributed command-line interface.
2. Depending on how many agents you plan to deploy with maximum security, issue the generateAgentId command to generate that number of unique agent IDs, output certificate signing requests (CSRs), and private keys.

   The command creates the following directories within the output directory that you specified:

- `\csr`: contains a CSR file, in base 64 binary encoded format, for each agent ID generated. The CSR files are named agent_ID.arm
- `\privkey`: contains a key file in PKCS#8 format for each CSR. The key files are named agent_ID.key and are protected by the specified password.

3. For each CSR, use your own Public Key Infrastructure (PKI) to do the following steps:
   - Get the request signed by a certificate authority to form an agent certificate.
   - Produce a PKCS12 keystore (agent_ID.p12) file, protected by a password, that contains the agent certificate, the private key, and the CA certificate. Set the friendly name to `itlm agent certificate`.
   - Import the certificate authority (CA) certificate to the Signer Certificate section of the ILMT truststore on the server.
   - Copy the keystore file to the directory on the server.
4. From the Asset Discovery for Distributed command-line interface, issue the convertcertificate command to convert the keystore file to a format supported by the security software used by the agent. For agents on Windows, Linux and UNIX platforms, the command converts the files found in the directory where you copied the keystore file to the CMS format (agent_ID.kdb) and stores them in the same directory. For agent on IBM i, the command converts the files to the keystore format and version that is supported by IBM i and stores them in the same directory.

   Note: If you deliver the agent certificate to the directory *Agent_Dir*`\keydb\private`, the agent, when started, will automatically import it.

```
generateAgentId -d directory -p privateKeyPassword -n numberOfIDs
convertcertificate -d directory -p p12Password -op cmsPassword
convertcertificate -d directory -p p12Password -op cmsPassword -os400 y
```

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 install 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.

Installing agents using native installers

Installation scripts or wizards are available for all supported platforms.

When installing the agent with the native installer, you can either use a response file to customize the installation parameters, or install the agent with the default values. Using the response file is recommended if you want to install the agents on multiple computers which have the same operating system and basic configuration - the file allows you to specify the parameters just once, and then export them to all your agents. If you decide not to use the response file, you will need to update some parameters in the `tlmagent.ini` configuration file after the installation.

Installing agents on Windows using a native installer

You can install agents on Windows platforms using an installation wizard. You can also use the installer to create a response file which you can later use to install agents on other Windows computers.

If you decided to install interactively, you will be using the installation wizard to specify a number of installation parameters. Ensure that none of the parameter values contain the character #, spaces or UTF strings. You can also use the installer to create an response file which you will later use to install agents on other Windows machines.

Note: The Asset Discovery for Distributed installer does not support file names with double-byte characters including log file names and response file names.

1. Log on to the computer where you want to install the agent as a user with administrative rights.
2. Click **setup.exe** to launch the installation wizard.
3. Select the language version that you want to install and click **Next**.
4. Select the installation type:

   Custom
   Allows you to specify all parameters.

   Typical
   Allows you to specify only the server address. It also enables you to save your settings in a response file. You can browse your file system and determine the directory where the response file is to be saved. All other agent parameters are set to default values.

   In this scenario, Custom is selected, showing the parameters that are available and their default settings.
5. Specify the agent parameters:

   Agent destination folder
   The folder in which the agent files will be installed. You can override the default installation path for the agent by changing the path shown here.

   Agent Temporary folder
   The folder in which the agent installer will store files during the installation process

   Common Inventory Tool, version 2.6 destination folder
   The folder in which the Common Inventory Technology files will be installed.

   Click **Next**.

6. On the **Connection security settings** panel specify the following agent parameters:

   Security level
   The level of security to be used when the agent plugs in to the server. Select one of the following values from the drop-down list.

   HTTP To use unsecure communication (minimal security).

   HTTPS Server Authentication
   To use secure communications with server authentication (medium security).

   HTTPS Server and Agent Authentication
   To use secure communications with client and server authentication (maximum security).

   Note:

   a. Agents with minimum and medium security levels can communicate with a server that has security levels of minimum or medium provided that both the secure and unsecure ports are configured. If the maximum security level is used, both the agent and the server must be aligned with the security level set to maximum.
   b. If you select medium or maximum security, you must set up and install the certificates. For full information about enabling security, see the "Security" section of the Tivoli Asset Discovery for Distributed information center.

   Use FIPS level of encryption
   Selecting this option enables use of FIPS-approved modules in the communication of encrypted data. The default is to not use FIPS-approved modules.

   Install certificate
   Selecting this option activates the **Certificate file** area in the lower part of the panel and enables the installation of security certificate.

   Use the embedded test certificate
   This option is selected by default (after you have selected the **Install certificate** check box). If you clear the check box, you will be able to use another certificate stored at a different location in the file system of the computer.

   Path to certificate file
   Click **Browse** to locate your new certificate file in the file system of your computer. You can override the embedded test certificate by defining the path to the chosen certificate here. The check box **Install certificate** should be selected.

   Click **Next**.
7. On the **Connection parameters** panel specify the following agent parameters:

   Server address
   The fully qualified host name or IP address of the server with which the agent is to communicate.

   Port This enables you to specify the port number that the agent will use to

communicate with the server. The default is 9988. If there is a star in front of port name, the corresponding security level has been selected on the previous pane.

Secure port
This enables you to specify the port number that the agent will use to communicate with the server if the **HTTPS Server Authentication** security level has been chosen. The default is 9999. If there is a star in front of port name, the corresponding security level has been selected on the previous pane.

Client Auth Secure port
This enables you to specify the port number that the agent will use to communicate with the server if the **HTTPS Server and Agent Authentication** security level has been chosen. The default is 9977. If there is a star in front of port name, the corresponding security level has been selected on the previous pane.

Use Proxy server
Select the check box if a proxy server is to be used in communications with the server. If you select this option, you must specify the proxy server address and port. The default is not to use a proxy server.

Proxy port
Specify the proxy server port if you have decided to use proxy server. The default proxy server port is 3128.

At this stage you might want to test the connection with the proxy server that you have defined. A **Test** button is available at the bottom of the panel.

Click **Next**.

8. On the **Advanced configuration** panel specify the following parameters:

   Max Cache Size
   The maximum size the agent cache can reach. Once this size is reached the oldest entries will be removed when new entries are added. The default is 2097152 bytes.

   Scan group
   The name of a scan group that the agent will belong to.

9. A summary panel opens. Select the check box **Install the agent**. If you plan to install 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.
10. When the installation is complete, click **Finish**.

Installing agents in silent mode:

Issue the following command: `start /wait setup /z"/sf<response_file> [/noprecheck]" /L<language> /s /f2"<silent_setup_log>"`. This command uses the following parameters:

<response_file>
The full path to the agent response file.

<language>
The code of the language that you want to use for installation. The following language codes are available:

- 1033 English (United States)
- 2052 Chinese (PRC)
- 1028 Chinese (Taiwan)
- 1036 French (France)
- 1031 German (Germany)
- 1040 Italian (Italy)
- 1041 Japanese
- 1046 Portuguese (Brazil)
- 1034 Spanish (Traditional Sort)
- 1042 Korean
- 1045 Polish
- 1049 Russian
- 1029 Czech
- 1038 Hungarian

<silent_setup_log>
The full path to the log file. This parameter is optional.

Installing agents on Linux using native installers

You can install agents on Linux platforms using the rpm command.

1. Copy the installer to a directory on 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 installer.
3. If you have downloaded the file from Passport Advantage, they are compressed. Uncompress the file and extract the installer files using the following command:

   ```
   tar xvzf <INSTALLER_COMPRESSED_FILE_NAME>.tar.gz
   ```

   In the directory you should have two files:
   - `ILMT-TAD4D-agent-7.2-linux-x86.rpm` (Linux x86), or
   - `ILMT-TAD4D-agent-7.2-linux-s390.rpm` (Linux 390), or
   - `ILMT-TAD4D-agent-7.2-linux-ppc.rpm` (Linux ppc), and
   - `ILMT_TAD4D_72_agentInstall_response.txt`
4. `ILMT_TAD4D_72_agentInstall_response.txt` is a template response file. If you want to install the agent with the response file, update the parameters in the file. See "UNIX agents installation response file" on page 106 for more information, and:
   - Rename the response file to `response_file.txt` and place it in your /etc directory. If the name of the file is different than `response_file.txt`, the file will not be read, or
   - Set the *LMT_RESPONSE_FILE_PATH* environment variable to point to the location of the response file.

   For example: `export LMT_RESPONSE_FILE_PATH=/tmp/response_file.txt`.

   Important: If you are installing the agent on Linux 390, you must use the response file to set the values in the **SharedPoolCapacity**, **SystemActiveProcessors** and **ProcessorType** parameters. If no values are specified, the installation will fail.
   You will be able to reuse the response file in any other agent installations on

systems with the same configuration. To do so, copy it to any machine where you want to reuse it and set the **LMT_RESPONSE_FILE_PATH** environment variable to point to its location or copy the response file to the `/etc` directory.

5. Enter the following command:

   ```
   rpm -ihv ILMT-TAD4D-agent-7.2-linux-x86.rpm
   ```

   or

   ```
   rpm -ihv ILMT-TAD4D-agent-7.2-linux-s390.rpm
   ```

   or

   ```
   rpm -ihv ILMT-TAD4D-agent-7.2-linux-ppc.rpm
   ```

   If no environment variable has been set, the installer automatically checks the /etc directory for the response file. If the file cannot be located, the agent is installed with the default parameters.
6. To verify that the installation has been successful, check if the agent appears as active in the Web interface. If the agent does not appear in the UI after several minutes, check the installation trace logs for information about possible errors. If the installation fails, the registry entry will state that the agent is installed. You need to run the agent uninstallation command.

If you installed the agent without the response file, it is configured to connect to a server located on the local host. If your server is installed on a different machine, use the `tlmagent -e` command to stop the agent, edit the server location parameter in the `tlmagent.ini` file:

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

then restart the agent using the `tlmagent -g` command. The `tlmagent.ini` file is located in the /etc directory.

Installing agents on AIX using native installers

You can install agents on AIX platforms using the installp command.

Before you begin

If you are installing agents on an AIX host that is partitioned using workload partitions (WPARs) with a logical partition (LPAR), you must install an agent in the LPAR before installing agents in the WPAR.

When installing agents with the native installer, you can either use a response file to customize the installation parameters, or install with default values. Using the response file is recommended if you want to install the agents on multiple computers with the same operating system and basic configuration, because you specify parameters such as server name and certificate names just once and then export them to all your agents.

If you decide not to use the response file, you will need to update some parameters in the `tlmagent.ini` configuration file after the installation.

If you install Common Inventory Technology in a workload partition in default location (`/opt`), you will have all the binaries shared with global AIX instance (LPAR) and also available to other workload partitions because by default `/opt`

directory is shared. Configuration files and Common Inventory Technology cache data are not shared between WPARs and the LPAR, and are always separate.

If you want to have a complete Common Inventory Technology installation inside a WPAR not sharing the binaries with the LPAR, you need to install Common Inventory Technology inside a WPAR in a directory (not shared between the LPAR and the WPAR) which has write permissions. This can be done by specifying **CITInstallPath** property in agent installation response file.

1. Copy the file for the installer from the directory on the installation DVD, or from the directory where you downloaded the software from IBM Passport Advantage to a directory on your computer. This is needed because the operating system generates the .toc file before starting the installation of the fileset.
2. Open a system command prompt and navigate to the directory where you stored the file.
3. If you have downloaded the file from Passport Advantage, uncompress the file by running the following command:

   ```
   gzip -d <INSTALLER_COMPRESSED_FILE_NAME>.tar.gz
   ```

   And extract the installer files by issuing the following command:

   ```
   tar xf <INSTALLER_TARBALL_FILE_NAME>.tar
   ```

   In the directory you should have two files:

   - `ILMT-TAD4D-agent-7.2-aix-ppc`
   - `ILMT_TAD4D_72_agentInstall_response.txt`
4. `ILMT_TAD4D_72_agentInstall_response.txt` is a template response file. Before installing the agent with the response file, update the parameters in the file, do the following steps:
   a. Optional: Edit the response file to customize its parameters to your situation.
   b. Rename the response file to `response_file.txt`.
   c. Either move the response file to your `/etc` directory, or set the *LMT_RESPONSE_FILE_PATH* environment variable to point to the location where the response file is stored. For example:

   ```
   export LMT_RESPONSE_FILE_PATH=/tmp/my_response_file.txt
   ```
5. To install the agent, issue the following command:

   ```
   installp -acgXd /tmp/TAD4D-agent/ILMT-TAD4D-agent-7.2-aix-ppc
   ```

   - In WPAR environments, the command is:

     ```
     installp -acgX -Or ILMT-TAD4D-agent
     ```

   If no environment variable has been set, the installer automatically checks the /etc directory for the response file. If the file cannot be located, the agent is installed with the default parameters.
6. To verify that the installation was successful, check if the agent appears as active in the Web interface. If the agent does not appear in the UI after several minutes, check the installation trace logs for information about possible errors.

If you did not use a response file, the agent is configured to connect to a server located on the local host. If your server is installed on a different computer, use the `stopsrc -s tlmagent` command to stop the agent, edit the server location parameter in the `tlmagent.ini` file:

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

Then, restart the agent using the `/usr/bin/startsrc -s tlmagent` command. The `tlmagent.ini` file is located in the /etc directory.

If your server is configured for the maximum security level, you need to import the agent certificate.

Installing agents on HP-UX using native installers

You can install agents on HP-UX platforms using the swinstall command.

1. Copy the installer to a directory on 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 installer.
3. If you have downloaded the file from Passport Advantage, uncompress the file by running the following command:

   ```
   gzip -d <INSTALLER_COMPRESSED_FILE_NAME>.tar.gz
   ```

   And extract the installer files by issuing the following command:

   ```
   tar xf <INSTALLER_TARBALL_FILE_NAME>.tar
   ```

   In the directory you should have two files:
   - `ILMT-TAD4D-agent-7.2-hpux_ia64`, or
   - `ILMT-TAD4D-agent-7.2-hpux_parisc`, and
   - `ILMT_TAD4D_72_agentInstall_response.txt`
4. `ILMT_TAD4D_72_agentInstall_response.txt` is a template response file. If you want to install the agent with the response file, update the parameters in the file. See "UNIX agents installation response file" on page 106 for more information, and:
   - Rename the response file to the `response_file.txt` and place it in your /etc directory. If the name of the file is different than `response_file.txt`, the file will not be read.

   You will be able to reuse the response file in any other agent installations on systems with the same configuration. To do so, copy it to the /etc directory on any machine where you want to reuse it.
5. To install the agent enter the following command:

   ```
   swinstall -s <ABSOLUTE_PATH_TO_INSTALLER_FILE>/ILMT-TAD4D-agent-7.2-hpux_ia64 ILMT-TAD4D-agent
   ```

   or

   ```
   swinstall -s <ABSOLUTE_PATH_TO_INSTALLER_FILE>/ILMT-TAD4D-agent-7.2-hpux_parisc ILMT-TAD4D-age
   ```

   To install the agent on HP-UX 11i v1, enter the following command:

   ```
   swinstall -s <ABSOLUTE_PATH_TO_INSTALLER_FILE>/ILMT-TAD4D-agent-7.2-hpux_ia64 -x enforce_depen
   ```

   The installer automatically checks the /etc directory for the response file. If the file cannot be located, the agent is installed with the default parameters.
6. To verify that the installation has been successful, check if the agent appears as active in the Web interface. If the agent does not appear in the UI after several minutes, check the installation trace logs for information about possible errors. If the installation fails, the registry entry will state that the agent is installed properly. You need to run the agent uninstallation command.

If you installed the agent without the response file, it is configured to connect to a server located on the local host. If your server is installed on a different machine, use the `tlmagent -e` command to stop the agent, edit the server location parameter in the `tlmagent.ini` file:

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

then restart the agent using the `tlmagent -g` command. The `tlmagent.ini` file is located in the /etc directory.

Installing agents on Solaris using native installers

You can install agents on Solaris platforms using the pkgadd command.

Note:

1. If you are installing agents on a Solaris platform that is partitioned using the Containers partitioning technology, you must install the agent in the global zone. The agent will automatically be installed also in all existing and future local zones.
2. If a Solaris platform is partitioned using the Containers partitioning technology, and you want to install an agent using the response file, you need to copy the `response_file.txt` files to the /etc directory on each zone (global and local). The environment variable LMT_RESPONSE_FILE_PATH that exists on the global zone is not visible on the local zones, so you cannot use it to install agents on the local zones.
3. Make sure that the status of agents on both zones is the same.If you are installing the agent for the first time, ensure that there are no agents already installed on either global or local zones.

1. Copy the installer to a directory on 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 installer.
3. If you have downloaded the file from Passport Advantage, uncompress the file by running the following command:

   ```
   gzip -d <INSTALLER_COMPRESSED_FILE_NAME>.tar.gz
   ```

   And extract the installer files by issuing the following command:

   ```
   tar xf <INSTALLER_TARBALL_FILE_NAME>.tar
   ```

   In the directory you should have two files:

   - `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`
4. `ILMT_TAD4D_72_agentInstall_response.txt` is a template response file. If you want to install the agent with the response file, update the parameters in the file. See “UNIX agents installation response file” on page 106 for more information, and:
   - Rename the response file to `response_file.txt` and place it in your /etc directory. If the name of the file is different than `response_file.txt`, the file will not be read, or
   - Set the *LMT_RESPONSE_FILE_PATH* environment variable to point to the location of the response file.

For example: `export LMT_RESPONSE_FILE_PATH=/tmp/response_file.txt`. You will be able to reuse the response file in any other agent installations on systems with the same configuration. To do so, copy it to any machine where you want to reuse it and set the *LMT_RESPONSE_FILE_PATH* environment variable to point to its location or place the response file in the `/etc` directory.

5. To install the agent enter the following command:

   ```
   pkgadd -d ILMT-TAD4D-agent-7.2-solaris-x86_64 ILMT-TAD4D-agent
   ```

   or

   ```
   pkgadd -d ILMT-TAD4D-agent-7.2-solaris-sparc32 ILMT-TAD4D-agent
   ```

   or

   ```
   pkgadd -d ILMT-TAD4D-agent-7.2-solaris-sparc64 ILMT-TAD4D-agent
   ```

   If no environment variable has been set, the installer automatically checks the /etc directory for the response file. If the file cannot be located, the agent is installed with the default parameters.
6. To verify that the installation has been successful, check if the agent appears as active in the Web interface. If the agent does not appear in the UI after several minutes, check the installation trace logs for information about possible errors. If the installation fails, the registry entries will state that the agent is properly installed. You need to run the agent unistallation command.

If you installed the agent without the response file, it is configured to connect to a server located on the local host. If your server is installed on a different machine, use the `tlmagent -e` command to stop the agent, edit the server location parameter in the `tlmagent.ini` file:

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

then restart the agent using the `tlmagent -g` command. The `tlmagent.ini` file is located in the /etc directory.

Installing agents on i5/OS using native installers

You can install agents on the i5/OS platform using the RSTLICPGM command.

Before you begin

You will require an IBM i user profile with authority to use the RSTLICPGM command

When installing agents with the native installer, you can use a response file to customize installation parameters such as the server address, or you can install with default values. Using the response file is recommended because you can reuse it to install the agents on other IBM i5/OS computers. If you do not provide a response file, the agent will be installed but you will need to edit the `tlmagent.ini` file on the IBM i host before the agent will start.

1. If you have downloaded the files from Passport Advantage, extract the installation package on a Windows computer.
2. Copy the SAVF file into a library on the target i5/OS computer. If you want to install the agent using the response file, you also need to copy the `ILMT_TAD4D_72_agentInstall_response.txt` file.

3. `ILMT_TAD4D_72_agentInstall_response.txt` is a template response file. If you want to install the agent with the response file, do the following steps:
   a. Update the parameters in the file. The server address (**MessageHandlerAddress**) is a mandatory parameter. See *The i5/OS agents installation response file* for more information.
   b. Rename the file to `os400_agent.txt` and place it in the /tmp/itlm.

   To use the same response file to install agents on other systems with the same configuration, copy the file to the `/tmp/tilm` directory on the target computer.
4. Log in to the node as user with authority to use the RSTLICPGM command.
5. To install the agent, enter the following command:
   ```
   RSTLICPGM LICPGM(1IBMTLM) DEV(*SAVF) RLS(V7R2M0) SAVF(<LIBRARY_WHERE_THE_SAVF_FILE_IS_PLACED>/<NA
   ```
   The installer automatically checks the /tmp/itlm directory for the response file. If the file cannot be located, the agent is installed with the default parameters.
6. To verify that the agent has been correctly installed, open the Installed License Programs panel on the OS/400® node, and check if there is an entry for 1IBMTLM.
7. If you installed the agent without a response file, specify the server address **<LMT_SERVER_NAME>** in the /QIBM/UserData/QITLM/conf/tlmagent.ini file and start the agent using the `strtcpsvr server(*itlmagent)` command.
8. To verify that the agent has started, check if it appears as active in the Web interface. If the agent does not appear in the UI after several minutes, check the installation trace logs for information about possible errors.

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.

Installing 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.

Agent installation response files

If you are installing the agents using the native installation tools, you can edit the response file to change the default installation parameters.

Windows agent installation response file and logon script configuration file

As an alternative to entering installation parameters interactively, you can create a response file for installing the Asset Discovery for Distributed agent on multiple Windows targets, or you can use a Windows logon script to install the agent

No response file is delivered with the product. To create one, use the native Windows installer, which is a wizard, long enough to generate the response file. A sample configuration file for logon scripts, `default.conf`, is provided.

Important: Do not use spaces, the number sign (#) , or UTF string in any parameter values. Also, do not include any non-Latin characters in any path names or scan group names.

Table 47. Windows agent installation parameters

Parameter	**Argument**	**Default**
	Description	
Setup: type	**SetupType**	Typical
	Select **Typical** to install the agent using default values for most of the parameters except **ScanGroup** and **MessageHandlerAddress**, both of which you must specify. Select **Custom** if you want to customize other parameters.	
Agent configuration: Scan group name	**ScanGroup**	DEFAULT
	The name of the scan group to which the agent will belong. The name cannot contain any special characters (e.g. spaces).	
Agent configuration: Message handler address	**MessageHandlerAddress**	localhost
	Specify the hostname or IP address of the Tivoli Asset Discovery for Distributed server. Message handler is a server component which manages incoming and outgoing agent data.	
Port	**Port**	9988
	Specify the port number used by the agent. This value is used for unsecure communications (SecurityLevel=0).	
Secure port	**SecureAuth**	9999
	Specify the port number used by the agent. This value is used for secure communications with server authentication (SecurityLevel=1).	

Table 47. Windows agent installation parameters (continued)

Parameter	**Argument**	**Default**
	Description	
Client Auth Secure Port	**SecureAll**	9977
	Specify the port number used by the agent. This value is used for secure communications with client and server authentication (SecurityLevel=2).	
Agent configuration: Agent installation path	**AgentInstallPath**	C:\WINDOWS\itlm
	To override the default location for agent installation, enter a valid path.	
Agent configuration: Agent temporary path	**AgentTempPath**	*YourTempDir*\itlm
	To override the location where agent keeps the working files, enter a valid path.	
Agent configuration: CIT destination path	**CITInstallPath**	C:\Program Files\Tivoli\cit
	Specify the Common Inventory Technology installation folder.	
Agent configuration: Maximum cache size	**MaxCacheSize**	2097152
	The maximum size the agent cache can reach in bytes. When this size is reached, the oldest entries will be removed as new entries are added. This value can be set between 50 and 15728640 bytes; a value outside of this range will prevent the agent from connecting to the Tivoli Asset Discovery for Distributed server.	
Agent configuration: Security level	**SecurityLevel**	0
	Determines the level of security to be used for communication between the agent and the Tivoli Asset Discovery for Distributed server. Possible values are: **0** To use unsecure communication. **1** To use secure communications with server authentication. **2** To use secure communications with client and server authentication. **Note:** 1. The Tivoli Asset Discovery for Distributed server configured for maximum security can communicate with agents set to maximum security only. If the server is configured to use medium security, then only agents set to medium or maximum security can connect to it. A server configured for minimum security can support agents set for any security level. 2. If you select medium (1) or maximum (2) security, you must perform a series of tasks to set up and install certificates. For full information about enabling security, see the "Security" section of the Tivoli Asset Discovery for Distributed infocenter.	
Agent configuration: FIPS enabled	**FipsEnabled**	false
	Specifies whether the agent is to use FIPS-approved modules in the communication of encrypted data. Possible values are *true* and *false*.	
Agent configuration: Use proxy	**UseProxy**	false
	Specifies whether the Tivoli Asset Discovery for Distributed server is protected by a proxy server. The following values are permitted: **true** The Tivoli Asset Discovery for Distributed server is protected by a proxy server. **false** The Tivoli Asset Discovery for Distributed server is not protected by a proxy server.	
Agent configuration: Proxy address	**ProxyAddress**	
	If **UseProxy** is *true*, enter the address (host name or IP address) of the proxy server.	
Agent configuration: Proxy port	**ProxyPort**	3128
	If **UseProxy** is *true*, enter the port of the proxy server.	

Table 47. Windows agent installation parameters (continued)

Parameter	Argument	Default
	Description	
Digital certificate: Install certificate	**InstallCertificate**	no
	If you have selected **SecurityLevel=1** or **SecurityLevel=2**, you can choose to install the server certificate. Possible values are *yes* and *no*. See the **CustomSSLCertificate** and **CertFilePath** description below.	
Digital certificate: Server custom certificate	**CustomSSLCertificate**	false
	If you have selected to supply server certificate (**installCertificate=yes**), you can choose to provide your own server certificate to be used by the agent for secure communications with the server. Permitted values are: **true** Indicates that you want to provide your own server certificate. **false** Indicates that you want to use the server test certificate. **Note:** The server test certificate can only be used for test purposes. Obtain your own certificate if secure communication is required in a live environment. If you select the value *true*, you must also supply the certificate pathname (**CertFilePath**).	
Digital certificate: Server certificate pathname	**CertFilePath**	
	If you have selected to supply a server certificate (**CustomSSLCertificate=true**), you must provide the pathname and filename of your own server certificate. The name of the certificate must be `cert.arm`. If the path contains spaces, enclose the whole path in double-quotes.	

UNIX agents installation response file

This table shows the installation parameters that you can edit in the UNIX agent installation response files.

Note: Do not use the character # in any of the agent parameters. Parameter values cannot include spaces or UTF strings.

You can find the response file in the following location: `/etc/response_file.txt`.

Table 48. UNIX agents installation parameters

Parameter	Argument	Default
	Description	
Port	**Port**	9988
	Specify the port number used by the agent. This value is used for unsecure communications (SecurityLevel=0).	
Secure Port	**SecureAuth**	9999
	Specify the port number used by the agent. This value is used for secure communications with server authentication (SecurityLevel=1).	
Client Auth Secure Port	**SecureAll**	9977
	Specify the port number used by the agent. This value is used for secure communications with client and server authentication (SecurityLevel=2).	
Agent configuration: Agent Installation Path	**AgentInstallPath**	/var/itlm
	To override the default location for agent installation, enter a valid path.	

Table 48. UNIX agents installation parameters (continued)

Parameter	Argument	Default
	Description	
Agent configuration: Agent Temporary Path	**AgentTempPath**	/tmp/itlm
	To override the location where agent keeps the working files, enter a valid path.	
Agent configuration: Message Handler Address	**MessageHandlerAddress**	localhost
	Specify the hostname or IP address of the Tivoli Asset Discovery for Distributed server. Message handler is a server component which manages incoming and outgoing agent data.	
Agent configuration: Scan Group Name	**ScanGroup**	DEFAULT
	The name of the scan group to which the agent will belong. The agent may be reassigned to another scan group by the Tivoli Asset Discovery for Distributed server, or by the inventory administrator on the server. The name of the scan group cannot contain any special characters (e.g. spaces).	
Agent configuration: Security level	**SecurityLevel**	0
	Determines the level of security to be used for communication between the agent and the Tivoli Asset Discovery for Distributed server. Possible values are: **0** To use unsecure communication. **1** To use secure communications with server authentication. **2** To use secure communications with client and server authentication. **Note:** 1. The Tivoli Asset Discovery for Distributed server configured for maximum security can communicate with agents set to maximum security only. If the server is configured to use medium security, then only agents set to medium or maximum security can connect to it. A server configured for minimum security can support agents set for any security level. 2. If you select medium (1) or maximum (2) security, you must perform a series of tasks to set up and install certificates. For full information about enabling security, see the "Security" section of the Tivoli Asset Discovery for Distributed infocenter.	
Agent configuration: Use Proxy	**UseProxy**	n
	Specifies whether the Tivoli Asset Discovery for Distributed server is protected by a proxy server. The following values are permitted: **y** The Tivoli Asset Discovery for Distributed server is protected by a proxy server. **n** The Tivoli Asset Discovery for Distributed server is not protected by a proxy server.	
Agent configuration: Proxy Port	**ProxyPort**	
	If **UseProxy** is *true*, enter the port of the proxy server.	
Agent configuration: Proxy Address	**ProxyAddress**	
	If **UseProxy** is *true*, enter the address (host name or IP address) of the proxy server.	
Agent configuration: FIPS Enabled	**FipsEnabled**	false
	Specifies whether the agent is to use FIPS-approved modules in the communication of encrypted data. Possible values are *true* and *false*.	
Agent configuration: Max Cache Size	**MaxCacheSize**	2097152
	The maximum size the agent cache can reach in bytes. When this size is reached, the oldest entries will be removed as new entries are added. This value can be set between 50 and 15728640 bytes; a value outside of this range will prevent the agent from connecting to the Tivoli Asset Discovery for Distributed server.	

Table 48. UNIX agents installation parameters (continued)

Parameter	Argument	Default
	Description	
Agent configuration: CIT Destination Path	**CITInstallPath**	
	Specify the Common Inventory Technology installation folder.	
Digital certificate: Install certificate	**InstallCertificate**	no
	If you have selected **SecurityLevel=1** or **SecurityLevel=2**, you can choose to install the server certificate. Possible values are *yes* and *no*. See the **CustomSSLCertificate** and **CertFilePath** descriptions below.	
Digital certificate: server custom certificate	**CustomSSLCertificate**	false
	If you have selected to supply server certificate (**InstallCertificate=yes**), you can choose to provide your own server certificate to be used by the agent for secure communications with the server. Permitted values are: **true** Indicates that you want to provide your own server certificate. **false** Indicates that you want to use the server test certificate. **Note:** The server test certificate can only be used for test purposes. Obtain your own certificate if secure communication is required in a live environment. If you select the value *true*, you must also supply the certificate pathname (**CertFilePath**).	
Digital certificate: server certificate pathname	**CertFilePath**	
	If you have selected to supply a server certificate (**CustomSSLCertificate=true**), you must provide the pathname and filename of the certificate. The name of the certificate must be `cert.arm`. If the path contains spaces, enclose the whole path in double-quotes.	
Linux 390: Node capacity	**SystemActiveProcessors**	
	If the Linux 390 image is running on IFL processors, this is the total number of IFL processors in the CEC. If the image is running on CP processors, this is the total number of CP processors in the CEC. This parameter is required for the installation to succeed.	
Linux 390: Shared pool capacity	**SharedPoolCapacity**	
	If the Linux 390 image is configured to share processors, specify the total number of shared processors in the CEC. Enter `0` if no shared processors are used by this image. This parameter is required for the installation to succeed. The value of this parameter cannot exceed the value of **SystemActiveProcessors**.	
Linux 390: Processor type	**ProcessorType**	
	Specify the processor brand on which the Linux image is running. Possible values are: **z9**® Your Linux image is running on System z9® or z990, or S/390®. **z10**™ Your Linux image is running on System z10™. This parameter is required for the installation to succeed.	
Solaris OS: Installation on Dynamic Domain	**InstallOnDD**	n
	If the agent is being installed on Dynamic Domain, this value should be set to true, otherwise to false. Permitted values are: **y** indicates that the agent is being installed on Dynamic Domain **n** Indicates that the agent is not being installed on Dynamic Domain	

Table 48. UNIX agents installation parameters (continued)

Parameter	Argument	Default
	Description	
Disable Rollback	**disableRollBack=yes**	
	Add this parameter to the response file to disable automatic rollback of changes to the system in case of a failed installation. This will preserve the failed installation on your computer, and allow you to examine it to discover the reasons for the failure.	

i5/OS agent installation response file

This table shows the installation parameters that you can edit in the i5/OS agent installation response files.

You need to create the installation response file in the following location: `/tmp/itlm/os400_agent.txt`. The following table provides a list of parameters that you can include in the file. All parameters except for **MessageHandlerAddress** are optional.

Note: Do not use the character # in any of the agent parameters. Parameter values cannot include spaces or UTF strings.

Table 49. i5/OS agents installation parameters

Parameter	Argument	Default
	Description	
Agent configuration: Port	**Port**	9988
	Specify the port number used by the agent. This value is used for unsecure communications (SecurityLevel=0).	
Agent configuration: Port	**SecureAuth**	9999
	Specify the port number used by the agent. This value is used for secure communications with server authentication (SecurityLevel=1).	
Agent configuration: Port	**SecureAll**	9977
	Specify the port number used by the agent. This value is used for secure communications with client and server authentication (SecurityLevel=2).	
Agent configuration: Message Handler Address	**MessageHandlerAddress**	
	Specify the hostname or IP address of the Tivoli Asset Discovery for Distributed server. Message handler is a server component which manages incoming and outgoing agent data. This is a mandatory parameter.	
Agent configuration: Scan Group Name	**ScanGroup**	DEFAULT
	The name of the scan group to which the agent will belong. The agent may be reassigned to another scan group by the Tivoli Asset Discovery for Distributed server, or by the inventory administrator on the server.	

Table 49. i5/OS agents installation parameters (continued)

Parameter	Argument	Default
	Description	
Agent configuration: Security level	**SecurityLevel**	0
	Determines the level of security to be used for communication between the agent and the Tivoli Asset Discovery for Distributed server. Possible values are: **0** To use unsecure communication. **1** To use secure communications with server authentication. **2** To use secure communications with client and server authentication. **Note:** 1. A Tivoli Asset Discovery for Distributed server configured for maximum security can communicate with agents set to maximum security only. If the server is configured to use medium security, then only agents set to medium or maximum security can connect to it. A server configured for minimum security can support agents set for any security level. 2. If you select medium (1) or maximum (2) security, you must perform a series of tasks to set up and install certificates. For full information about enabling security, see the "Security" section of the Tivoli Asset Discovery for Distributed infocenter.	
Agent configuration: Use Proxy	**UseProxy**	n
	Specifies whether the Tivoli Asset Discovery for Distributed server is protected by a proxy server. The following values are permitted: **y** The Tivoli Asset Discovery for Distributed server is protected by a proxy server. **n** The Tivoli Asset Discovery for Distributed server is not protected by a proxy server.	
Agent configuration: Proxy Port	**ProxyPort**	
	If **UseProxy** is *true*, enter the port of the proxy server.	
Agent configuration: Proxy Address	**ProxyAddress**	
	If **UseProxy** is *true*, enter the address (host name or IP address) of the proxy server.	
Agent configuration: Max Cache Size	**MaxCacheSize**	2097152
	The maximum size the agent cache can reach in bytes. When this size is reached, the oldest entries will be removed as new entries are added. This value can be set between 50 and 15728640 bytes; a value outside of this range will prevent the agent from connecting to the Tivoli Asset Discovery for Distributed server.	
Digital certificate: Install certificate	**InstallCertificate**	no
	If you have selected **SecurityLevel=1** or **SecurityLevel=2**, you can choose to install certificates. Possible values are: **yes** Install server certificate defined in **CertFilePath** or agent certificate defined in **PrivateCertFilePath**, or both. If **CertFilePath=none**, the server test certificate will be installed. **no** Do not install any certificate file.	

Table 49. i5/OS agents installation parameters (continued)

Parameter	Argument	Default
	Description	
Digital certificate: server certificate pathname	**CertFilePath**	
	If you have selected to supply certificates (**installCertificate=yes**), you can choose to provide your own server certificate to be used for server authentication by the agent (**SecurityLevel>0**). Possible values are: `<path>/cert.arm` - Indicates that you want to provide your own server certificate. none - Indicates that you want to use the server test certificate. The name of the server certificate must be `cert.arm`. If the path contains spaces, enclose the whole path in double-quotes. **Note:** The test certificate may only be used for test purposes as it is in the name of IBM and is insecure (the same certificate is distributed to all customers).	
Digital certificate: agent certificate pathname	**PrivateCertFilePath**	none
	If you have selected to supply certificates (**installCertificate=yes**), you can provide the pathname of CMS keystore which contains the agent certificate. The password for this keystore must be set to `slmtest`. If the path contains spaces, enclose the whole path in double-quotes.	

Agent installation software package blocks

If you are installing the agent using Configuration Manager, you can edit the software package parameters to customize your installation.

Software package parameters for UNIX and Windows platforms

This table lists the parameters for deploying Tivoli Asset Discovery for Distributed agent on Linux, UNIX and Windows platforms using TivoliConfiguration Manager.

Table 50. Configuration parameters in the agent software package blocks

Parameter name	Description
scanGroup	The name of a scan group that has been created in the Tivoli Asset Discovery for Distributed server database.
useProxy	Set to *y* if a proxy port is to be used for communications between agents and the Tivoli Asset Discovery for Distributed server. The default is *n*.
proxyName	The fully qualified host name or IP address of the proxy server, if applicable.
proxyPort	The port number on which the proxy server listens, if applicable.
serverAddress	The fully qualified host name or IP address of the Tivoli Asset Discovery for Distributed server with which the agent is to communicate. The default is *localhost*.

Table 50. Configuration parameters in the agent software package blocks (continued)

Parameter name	Description
security_level	The level of security to be used for communication between the agent and the Tivoli Asset Discovery for Distributed server. Valid values are: **0** To use unsecure communication. **1** To use secure communications with server authentication. **2** To use secure communications with client and server authentication. **Note:** 1. A Tivoli Asset Discovery for Distributed server configured for maximum security can communicate with agents set to maximum security only. If the server is configured to use medium security, then only agents set to medium or maximum security can connect to it. A server configured for minimum can support agents set for any security level. 2. If you select medium or maximum security, you must perform a series of tasks to set up and install certificates. For full information about enabling security, see the "Security" section of the information center.
target_dir	The name of the directory on the endpoint that is used by the software package block to unpack its file images. The default is the temporary directory.
fips_enabled	Set to *y* to enable encryption of data using a FIPS-approved algorithm. The default is *n*.
installCertificate	Set to *no* if you do not want to have a server certificate installed as part of the distribution. The default is *no*. You can install server test certificate without installing agent certificate by providing the following parameters: **installCertificate=yes**, **certificate_path=none** , and **privateCertificate=none**.
certificate_path	If you have selected to supply certificates (**installCertificate=yes**), you can choose to provide your own server certificate to be used for server authentication by the agent (**SecurityLevel>0**). Possible values are: `<path>/cert.arm` - Indicates that you want to provide your own server certificate. none - Indicates that you want to use the server test certificate. The name of the server certificate must be `cert.arm`. If the path contains spaces, enclose the whole path in double-quotes. **Note:** The test certificate may only be used for test purposes as it is in the name of IBM and is insecure (the same certificate is distributed to all customers).
privateCertificate	If you have selected to supply certificates (**installCertificate=yes**) and you are using security level 2, you need to specify the path to CMS keystore which contains the agent certificate, specific to the agent that is to be deployed. The password of this keystore must be set to `slmtest`. The default value of this parameter is *none*.
max_cache_size	The maximum size the agent cache can reach. Once this size is reached the oldest entries will be removed when new entries are added. The default is 2097152 (bytes).

Table 50. Configuration parameters in the agent software package blocks (continued)

Parameter name	Description
agt_install_path	The path where the agent is to be installed. The default value depends on the platform.
agt_tmp_path	The location of temporary agent files on the agent computer. The default value depends on the platform. For more information, see the related reference section.
agt_pkg_dir	Super Software Package Blocks uncompress all their Software Package Blocks files there.
agt_temp_dir	Software Package Blocks use this folder to store temporary files.
DisableRollBack	When the installation is unsuccessful a rollback will be started automatically. The default is *no*.
CheckDiskSpace	The variable determines if the installer is to check the amount of free space on the target drive. The default is *yes*.
processorType (Linux for zSeries only)	The processor brand on which the Linux for zSeries image is running. **z9** The Linux for zSeries image is running on System z9 or z990 or S/390. **z10** The Linux for zSeries image is running on System z10.
sharedPoolCapacity (Linux for zSeries only)	The total number of shared processors in the computer. The default is *0*.
systemActiveProcessors (Linux for zSeries only)	The total number of processors in the computer. The default is *0*.

Software package parameters for IBM i

The following table lists the parameters included in the IBM i agent software package blocks and gives guidelines for the values to be supplied.

Note: Do not use the character # in any of the agent parameters.

Table 51. Configuration parameters in the agent software package blocks

Parameter name	Description
proxyPort	The port number on which the proxy server listens, if applicable. The default is *8080*.
useProxy	Set to *y* if a proxy port is to be used for communications between agents and the Tivoli Asset Discovery for Distributed server. The default is *n*.
scanGroup	The name of a scan group that has been created in the Tivoli Asset Discovery for Distributed server database. The default is *DEFAULT*.
port	Specify the port number used by the agent. This value is used for unsecure communications (SecurityLevel=0).
secure_port	Specify the port number used by the agent. This value is used for secure communications with server authentication (SecurityLevel=1).
serverAddress	The fully qualified host name or IP address of the Tivoli Asset Discovery for Distributed server with which the agent is to communicate. The default is *localhost*.
client_auth_ secure_port	Specify the port number used by the agent. This value is used for secure communications with client and server authentication (SecurityLevel=2)

Table 51. Configuration parameters in the agent software package blocks (continued)

Parameter name	Description
security_level	Determines the level of security to be used for communication between the agent and the Tivoli Asset Discovery for Distributed server. Valid values are: **0** To use unsecure communication. **1** To use secure communications with server authentication. **2** To use secure communications with client and server authentication. **Note:** 1. A Tivoli Asset Discovery for Distributed server configured for maximum security can communicate with agents set to maximum security only. If the server is configured to use medium security, then only agents set to medium or maximum security can connect to it. A server configured for minimum security can support agent set for any security level. 2. If you select medium or maximum security, you must perform a series of tasks to set up and install certificates. For full information about enabling security, see the "Security" section of the Tivoli Asset Discovery for Distributed infocenter. The default is *0*.
max_cache_size	The maximum size the agent cache can reach in bytes. When this size is reached, the oldest entries will be removed as new entries are added. This value can be set between 50 and 15728640 bytes; a value outside of this range will prevent the agent from connecting to the Tivoli Asset Discovery for Distributed server.
proxyName	The fully qualified host name or IP address of the proxy server, if applicable.
installCertificate	Set to *yes* if you want to have a server certificate installed as part of the distribution. The default is *no*. You can install server test certificate without installing agent certificate by providing the following parameters in the response file: **installCertificate=yes**, **privateCertificate=none**, and **certificate_path=none**.
certificate_path	If you have selected to supply certificates (**installCertificate=yes**), you can choose to provide your own server certificate to be used for server authentication by the agent (SecurityLevel>0). Possible values are: `<path>/cert.arm` - Indicates that you want to provide your own server certificate. none - Indicates that you want to use the server test certificate. It is the default value. The name of the server certificate must be `cert.arm`. If the path contains spaces, enclose the whole path in double-quotes. **Note:** The test certificate may only be used for test purposes as it is in the name of IBM and is insecure (the same certificate is distributed to all customers).

Table 51. Configuration parameters in the agent software package blocks (continued)

Parameter name	Description
privateCertificate	If you have selected to supply certificates (**installCertificate=yes**) and you are using security level 2, you can specify the path to CMS keystore which contains agent certificate, specific to the agent that is to be deployed. The password of this keystore must be set to `slmtest`. The default value for this parameter is *none*.

Uninstalling

This section provides instructions for uninstalling the Tivoli Asset Discovery for Distributed servers, database and agents.

Uninstalling the Tivoli Asset Discovery for Distributed servers and databases

The uninstall wizard identifies the server and database elements that are installed on a computer and enables you to select those that you want to uninstall. If a database element is installed on the computer, the wizard gives you the option of dropping the database.

You need to uninstall the product before you can install it again on the same machine. Simply removing the files or dropping the database is not enough to complete the installation.

If you are uninstalling the database element to move it to a different computer and you want to retain the data held in the database, make a back up of the database before uninstalling, then restore the backup to populate the database that you have installed on the new computer. See *Moving a database* for more information.

If you are uninstalling from a computer where Windows Terminal Services is installed, you must change to install mode before launching the wizard.

Uninstalling the server in interactive mode

The interactive uninstallation mode lets you use the uninstallation wizard to specify the parameters for the uninstallation step by step.

Before you begin

The interactive uninstallation mode requires your machine to have a GUI. For UNIX platforms, ensure that your machine has a graphical user interface such as X Window.

To do this:

The uninstall wizard is located in the folder *INSTALL_DIR*`\_uninst`. On UNIX platforms, there is a folder called `deinstl`. This folder is not the uninstall folder. It contains files used in the uninstallation.

1. Start the uninstall wizard (Windows) or `uninstaller.bin` (UNIX).
   a. Select the **Add/Remove Programs** option from the Control Panel.
   b. Select **Hardware and Software Identification for Distributed**.
   c. Click **Remove**.
2. From the drop-down list, select the language to be used by the wizard.

3. The wizard detects the elements that are present on the computer. Deselect any that you do not wish to uninstall.
4. Select the option to drop the database tables if appropriate.

   If an error is generated when attempting to drop the database, you can manually drop the database using the DB2 command `db2 drop database tlma`, where *tlma* is the name of the Tivoli Asset Discovery for Distributed database.
5. The wizard displays a panel showing the elements to be uninstalled. Click **Next** to commence the uninstallation.
6. Click **Next** to continue the uninstallation.
7. When the uninstallation is complete, click **Finish** to exit from the wizard.

You have uninstalled the Tivoli Asset Discovery for Distributed server and database.

The wizard does not uninstall the DB2 database, or delete any user group created during the DB2 installation. You need to delete these groups manually.

In order to delete the Tivoli Asset Discovery for Distributed logs you have to delete the contents of the Tivoli Common Directory (provided that no other IBM Tivoli application uses that folder to store its logs).

Uninstalling the server in silent mode

When the uninstall wizard runs in silent mode, it takes the parameters it requires from an InstallShield response file.

The response file, `uninstallresponse.txt`, is provided in the *INSTALL_DIR*`\_uninst` directory. You need to edit this file to provide the values for parameters that the wizard sets. See *The server and database uninstallation response file* for a full description of the file.

The uninstall wizard is located in the folder *INSTALL_DIR*`\_uninst`. On UNIX platforms, there is a folder called `deinstl`. This folder is not the uninstall folder. It contains files used in the uninstallation.

Use the command-line interface to launch the wizard in silent mode.

1. Log on the computer where you want to run the wizard with Administrator or root rights.
2. Navigate to the *INSTALL_DIR*`\_uninst` directory and open the `uninstallresponse.txt` file.
3. Edit the response file so that the parameters describe the uninstallation that you want to perform.
4. From the command-line interface, launch the wizard's uninstall script (`uninstaller.exe` for Widows and `uninstaller.bin` for other platforms) with the following arguments:

   –options "*INSTALL_DIR*_uninst\uninstallresponse.txt" –silent

The Tivoli Asset Discovery for Distributed uninstallation wizard runs in silent mode.

The wizard does not uninstall the DB2 database, or delete any user group created during the DB2 installation. You need to delete these groups manually.

In order to delete the Tivoli Asset Discovery for Distributed logs you have to delete the contents of the Tivoli Common Directory (provided that no other IBM Tivoli application uses that folder to store its logs).

The server and database uninstallation response file:

The `uninstallresponse.txt` file, which is provided with Tivoli Asset Discovery for Distributed, is an InstallShield options file. It defines arguments to set each parameter required by the Tivoli Asset Discovery for Distributed uninstallation wizard.

Table 52. Server and database silent uninstall parameters

Parameter	Parameter key name	Default
	Description	
Uninstall Tivoli Asset Discovery for Distributed server element	-P admin.activeForUninstall=	true
	Specifies whether or not the Tivoli Asset Discovery for Distributed element should be uninstalled. Possible values are: **true** The server will be uninstalled. **false** The server will not be uninstalled. This parameter will be ignored if the server is not installed on the computer.	
Uninstall Tivoli Asset Discovery for Distributed database element	-P adminDB.activeForUninstall=	true
	Specifies whether or not the Tivoli Asset Discovery for Distributed database should be uninstalled. Possible values are: **true** The database will be uninstalled. **false** The database will not be uninstalled. This parameter will be ignored if the element is not installed on the computer.	
Uninstalling databases: drop database	-W uninstallFeature.dbDropping=	false
	Specifies whether or not any Tivoli Asset Discovery for Distributed databases on this computer should be deleted. Possible values are: **true** The databases will be dropped. **false** The databases will not be dropped.	
The bundled WebSphere Application Server user ID	-W was_credential.UserId=	
	If you are uninstalling a server that is running within a WebSphere Application Server secure cell, supply the user ID to be used to authenticate access to the cell.	
The bundled WebSphere Application Server password	-W was_credential.Pwd=	
	If you are uninstalling a server that is running within a WebSphere Application Server secure cell, supply the password to be used to authenticate access to the cell.	

Running scripts to uninstall Tivoli Asset Discovery for Distributed

You can uninstall the Tivoli Asset Discovery for Distributed server applications using the scripts provided by IBM. They are model scripts and you can modify them so that they reflect your infrastructure and your specific needs.

Before you begin

1. You need to have the **setupWAS.properties** file filled with the same parameters as those used during the deployment phase. See the topic *Editing the setupWAS.properties file*.

2. You need to have the following scripts and files in one directory, for example **WAS-scripts** directory:
   - `cleanupDataSources.jacl`
   - `cleanupServerSecurePorts.jacl`
   - `cleanupWAS.bat`
   - `cleanupWAS.sh`
   - `setupWAS.properties`
   - `undeployAdmin.jacl`
   - `undeployAdminCommon.jacl`
   - `undeployMessageHandler.jacl`

   You can extract the files using the Tivoli Asset Discovery for Distributed interactive installer.

To do this:

1. Open the command line prompt, and enter the directory which contains your installation scripts, for example **WAS-scripts**.
2. Run the following command with the path to the correct profile that you want to undeploy Tivoli Asset Discovery for Distributed from:
   - Windows **cleanupWAS.bat** *PATH_TO_THE_PROFILE* [-force] [-log log_file_path] where **-force** continues on errors, and **-log** logs you into a given file (default log file: SetupWAS.log in current directory).
   - UNIX **cleanupWAS.sh** *PATH_TO_THE_PROFILE* [-f] [-l log_file_path] where **-f** continues on errors, and **-l** logs you into a given file (default log file: SetupWAS.log in current directory).

   The command starts various undeployment scrips. For information about the function of each of the scripts used see *Scripts used in undeploying the server on WebSphere Application Base version*. Wait until the scripts finish; this may take a few minutes depending on the capacity of your machine.
3. After successfully undeploying the applications restart the WebSphere Application Server.

- Windows **cleanupWAS.bat** `C:\Program Files\IBM\WebSphere\AppServer`
- UNIX **cleanupWAS.sh** `/opt/IBM/WebSphere/AppServer`

Scripts used in undeploying the server on WebSphere Application stand-alone version

This topic lists the script files that are used in undeploying Tivoli Asset Discovery for Distributed. It also describes their function in the process.

Table 53. Tivoli Asset Discovery for Distributed undeployment script files

Script file	Function
undeployAdmin.jacl	The script uninstalls administration component.
undeployAdminCommon.jacl	The script uninstalls other files used by the administration component.
undeployMessageHandler.jacl	The script uninstalls the Message Handler component.
cleanupDataSources.jacl	The script deletes the JDBC Provider name.
cleanupServerSecurePorts.jacl	The script removes port numbers used for secure communication.
cleanupTimerManager.jacl	The script removes timer managers.

Uninstalling the agents

You can uninstall the agents either with the native installation tools for your system, or using the **tlmunins** script. The native installation tools method is only available if the agents were also installed in the same way, and not upgraded using the self-update method.

Uninstalling Tivoli Asset Discovery for Distributed agents using the tlmunins script

You can use the tlmunins script to uninstall all Windows and UNIX agents, regardless of the method used to install them. The script is not available for IBM i agents.

1. Navigate to the directory where the agent is installed.
2. Run the uninstallation script.
   - On Windows, run `tlmunins.bat`.
   - On UNIX platforms, run `tlmunins.sh`.

If an agent was installed using native tools, the `tlmunins` script will automatically run an appropriate native tool to remove the agent.

To complete the uninstallation, delete the agent installation directory and remove the agent in the administration console.

Uninstalling agents using native installation tools

If you installed the agent using the native installation tools for your platform, you can uninstall it in the same way.

You cannot use the native installation tools to remove an agent that was installed via another installation method, or upgraded using self-update. To uninstall those agents, see *Uninstalling agents using the tlmunins script*.

The exact uninstallation methods depend on the platform on which the agent is installed.

If the agent was installed using native tools, the tlmunins script will automatically run appropriate native tool to remove the agent.

Uninstalling AIX agents:

Uninstall AIX agents using the installp command.

1. Open a system command prompt.
2. Enter the following command:

```
installp -u ILMT-TAD4D-agent
```

To complete the uninstallation, you need to remove the agent in the administration console. See *Removing agents in the administration console* for more information.

Uninstalling HP-UX agents:

Uninstall HP-UX agents using the swremove command.

1. Open a system command prompt.
2. Enter the following command:

```
swremove ILMT-TAD4D-agent
```

To complete the uninstallation, you need to remove the agent in the administration console. See *Removing agents in the administration console* for more information.

Uninstalling IBM i agents:

Uninstall IBM i agents using the IBM i function Delete Licensed Program.

Before you begin

Stop the agent before uninstallation.

1. Open a system command prompt.
2. Enter the following command:
   ```
   DLTLICPGM LICPGM(1IBMTLM)
   ```

To complete the uninstallation, you need to remove the agent in the administration console. See *Removing agents in the administration console* for more information.

After uninstalling the agent, some agent files still remain on your disk, including the `tlmagent.ini` file. This is why installing the agent again is considered an upgrade of the agent and not a pristine installation. To fully uninstall the agent after executing the `DLTLICPGM` command, the `/QIBM/UserData/QITLM` directory needs to be removed manually.

Uninstalling Linux agents:

Uninstall Linux agents using the rpm command.

1. Open a system command prompt.
2. Enter the following command:
   ```
   rpm -e ILMT-TAD4D-agent
   ```

To complete the uninstallation, you need to remove the agent in the administration console. See *Removing agents in the administration console* for more information.

Uninstalling Solaris agents:

Uninstall Solaris agents using the pkgrm command.

When you uninstall the agent in a global zone, all agents installed in local zones set in this global one will also be uninstalled.

1. Open a system command prompt.
2. Enter the following command:
   ```
   pkgrm ILMT-TAD4D-agent
   ```

To complete the uninstallation, you need to remove the agent in the administration console. See *Removing agents in the administration console* for more information.

Uninstalling Windows agents:

Uninstall Windows agents using the uninstallation wizard.

1. Start the uninstall wizard.
   a. Select the **Add/Remove Programs** option from the Control Panel.
   b. Select **ILMT-TAD4D Agent version 7.2**.
   c. Click **Remove**.

2. Click **OK** to commence the uninstallation.
3. When the uninstallation is completed, click **Finish** to exit from the wizard.

To complete the uninstallation, you need to remove the agent in the administration console. See *Removing agents in the administration console* for more information.

Removing agents

You have the possibility of removing agents, for example inactive agents, from the table.

Note: Removing an agent means unregistering it from the server; it does not mean that the agent is uninstalled.

Before you begin

You must be an inventory administrator to perform this task.

1. In the navigation bar, click **Infrastructure** → **Agents**.
2. Choose one or more agents by selecting the check boxes.
3. From the **Select Action** list, choose **Remove**, then click **Go**.

   Important: You should perform all the actions pertaining to bundling before you remove the agents.

Removing inactive agents

Removing inactive agents means that the agent information is removed from the server, and thus from the table. This process also influences the overall agent status on the Home page. Note that you will still be able to see the agent information in, for example, old audit reports.

Removing active agents

If you **remove** an active agent, for example by accident, it will automatically register back the next time it contacts the server (and again appear in the table).

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 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.

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 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 54. 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 55. 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
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.

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 56. 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 57. 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

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 123 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.

Common Inventory Technology information

If problems occur with the Common Inventory Technology component of the product, you can use the return codes for troubleshooting.

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 58. 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 58. 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 58. 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 58. 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 58. 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 58. 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 58. 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 58. 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 58. 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 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.

Server operation and CLI problems

This topic explains how to solve some common problems with the server and the command-line interface.

Table 59. Problems and solutions for the server and command line interface

Problem	Potential solution
Unable to connect from the Web UI to a given VM manager.	Check if the connection with the VM manager is active by performing one or more of the following actions: 1. Check if the Web address of a VM manager ends with `/sdk`. 2. Try using either `http` or `https` in the **Web address** field. 3. Check if the URL of a given VM manager is active in the browser on the server machine (by adding `/mob` at the end of the URL).
When trying to run the server command-line interface (CLI) on Windows platforms it issues an error that the system cannot find the path specified.	This occurs when cygwin is installed. You must remove cygwin from the environment variable PATH.
A command fails with a "CODCL7571E: Server connection error" message	Verify the following: • The server to ensure it is working • Security is configured on the server • You can ping localhost (CLI connects to server on localhost) If it appears during a software catalog import using the CLI, the import status can be checked on the Import Software Catalog UI page.
The server has become isolated from the database	This can occur when the time zone or the time set on the administration server is not aligned with the time zone or the time on the database. To solve this problem stop and restart the database to align the time zone and time set on the administration servers with their database.
The server cannot connect to the database	Verify the following: • The logs to make sure no errors have occurred. • The administration server is up and running, and connecting through the GUI interface. • The database is up and running and, if it is a remote database, that the network connection is working. • The firewall is not blocking the local connection
The `viewer` command fails on Linux platforms for IBM zSeries if it is issued with the parameter `-s text`.	The trace formatter is not correctly specified. To use viewer command, the trace formatter must be specified in the `log.properties` file: `itlm.traceformatter.className=com.ibm.log.PDXMLFormatter`
A command fails with a "No space on device" message.	This message is generated by the command line logging component when there is no space in the directory where it is logging.
Server communication is unsuccessful following the configuration of SSL.	The certificate has not been correctly created or distributed. If there is any problem with the certificates used to authenticate secure communications, exceptions reporting authentication errors are logged in the SSL error log of the HTTP server on the server side and in the trace log on the client side. If you find these log entries, you must check that you have correctly followed the procedures for requesting or creating certificates.

Table 59. Problems and solutions for the server and command line interface (continued)

Problem	Potential solution
After changing the system date you can not use the CLI.	When the system date is changed you should regenerate and replace the existing certificate and then stop and start the system server.
Server Web interface cannot connect to the database.	Some causes of this error can be identified using the pdtool command. Problems with the level or configuration of JDBC driver, the configuration of the database, or of the database pooler cause messages, which describe the cause and solution of the problem, to be recorded in the server message log and these messages will be identified and extracted by the pdtool command. If the problem is not identified by the pdtool command, it might be caused by one of the following situations: • DB2 services were not running during the installation process or were started after the embedded WebSphere Application Server started. You will need to do the following: 1. Stop the server. 2. Stop the embedded WebSphere Application Server. 3. Stop DB2. 4. Uninstall the database component. 5. Start DB2. 6. Start the embedded WebSphere Application Server. 7. Reinstall the database. • The install wizard did not successfully create and populate the database. On the computer where the database is installed, you will need to run the uninstall wizard to uninstall the database component and then reinstall it.
DB2 communication error occurs when a filtered query is submitted for a report.	On Windows platforms, the query fails and a message indicating a DB2 communication error occurs when a report is submitted that includes filtered parameters, for example, if the report is to include only products whose names include a specified string. This error is caused by agent stack size overflow. You can resolve it by increasing the DB2 database configuration parameter, `AGENT_STACK_SZ` to **100**.
Server starts in problem determination mode.	If you have the server and database installed on separate computers, ensure that their clocks are synchronized. Use a non-manual method of clock synchronization, for example Network Time Protocol.
Report signing fails.	There might not be enough space in the directory where the report is generated. 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. You can specify another location where the XML file should be generated by editing the **reportPath** parameter in the `system.properties` file.

Table 59. Problems and solutions for the server and command line interface (continued)

Problem	Potential solution
Database transaction log is overflowing.	See "Configuring the transaction log size" on page 157 for possible solution.

Server is running, but an exception in traces appears. The exception is related to the connection with the specified ESX with the following message: `"javax.net.ssl.SSLException: Unrecognized SSL message, plaintext connection?"`	1. Add the following lines to file `/etc/vmware/hostd/config.xml`:
	`..`
	`<ssl>`
	`<doVersionCheck> false </doVersionCheck>`
	`<handshakeTimeoutMs>30000</handshakeTimeoutMs>`
	`</ssl>`
	`<http>`
	`<readTimeoutMs>45000</readTimeoutMs>`
	`<writeTimeoutMs>45000</writeTimeoutMs>`
	`<blacklistPeriodMs>3000</blacklistPeriodMs>`
	`</http>`
	`<vmdb>`
	`...`
	2. Restart the hostd service using `service mgmt-vmare restart`.
	3. Verify that the exception does not occur.

Server is running, but an `org.xml.sax.SAXParseException` exception in traces appears. The exception is related to the connection with the specified ESX.	Make sure you have the latest patches to your problematic ESX server installed.
On SUSE Linux Enterprise Server 10 SP 2, Power 64 bit, when the <installationPath>/cli/srvstop.sh command is run, the following exception in traces is returned: `Exception in thread "main" java.lang.UnsatisfiedLinkError: /opt/IBM/LMT/eWAS/java/jre/bin/xawt/libmawt.so (libX11.so.6: cannot open shared object file: No such file or directory).`	The X11 X.org libraries in 64-bit version are missing. Install the package xorg-x11-libs-64bit compatible with the version of SUSE Linux Enterprise Server 10 that you use. For SUSE Linux Enterprise Server 10 SP 2, Power 64 bit, the libraries are available in the package: xorg-x11-libs-64bit-6.9.0-50.58.ppc.rpm. The package has the following dependencies: 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.
Server is running and security is turned on. The command <installationPath>/cli/srvstop.sh is run, and the following error appears: `X connection to localhost:13.0 broken (explicit kill or server shutdown).`	If you want to stop the server on which security is turned on, and the X server is not available, you should use the appropriate parameters described in the ../com.ibm.license.mgmt.admin.doc/t_server_stop.dita section.
Automatic report generation fails. If the gap between the end date of the last signed report and the start date of automatic report generation (set in the Reporting Options window) is bigger than 3 months, the reports are not generated automatically.	To solve this situation, create manually some reports so that the gap is shorter than 3 months, and sign them.

Agent installation and upgrade problems

This topic explains how to solve some common problems while installing and upgrading the agent.

Table 60. 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
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`

Table 60. Problems and solutions for agent installation and upgrade (continued)

Problem	Potential solution
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.
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.

Table 60. Problems and solutions for agent installation and upgrade (continued)

Problem	Potential solution
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.
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.

Table 60. Problems and solutions for agent installation and upgrade (continued)

Problem	Potential solution
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.
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.

Agent operation problems

For some agent problems, the symptom is detected at the server. For others, the system administrator might receive a communication from the user on whose system the agent is running. Some solutions require the application user to take some action, such as enter a specific command.

Table 61. Problems and solutions with the agent

Problem	Potential solution
During software scans, an agent accesses the shared file system, which is an undesired behavior and it can cause high CPU consumption, hanging or crashing of the scanner.	To solve the situation: • Use the **scan_exclude_dirs** parameter to prevent the problematic drive from being scanned. If a specific shared file system is mounted by an automount facility, use the **assume_auto_fs=remote** parameter to skip it. To view more information about this task, see: Excluding agent directories from being scanned.

Table 61. Problems and solutions with the agent (continued)

Problem	Potential solution
Agent status is *inactive*.	There are four main reasons for the agent to be *inactive*: 1. Agent is not running - to resolve this problem, start the agent service, using the following command: • On Windows - `<AGENT_INSTALL_DIR>\tlmagent -g` • On AIX - `/usr/bin/startsrc -s tlmagent` • On i5/OS - `strtcpsvr server(*itlmagent)` • On other platforms - `<AGENT_INSTALL_DIR>/tlmagent -g` 2. Agent was uninstalled - check if it is installed; if it is installed you should be able to localize `tlmagent` binary file in the agent installation directory. 3. The security level is higher on the server than on the agents. Check the security levels: • Agent's security level is defined in `tlmagent.ini`. • Server's security level is defined in DB2 in `lic.control_values table`. To learn how to change the security level, see: Upgrading from minimum to medium security or Upgrading from medium to maximum security. 4. There is no communication between the agent and the server - see: *The agent fails to contact the administration server* problem below in this table. You may also check the log files to find the potential problems. These files are created in the following directories: • **Message files** - `<TIVOLI_COMMON_DIRECTORY>/COD/logs/agent/message`, for example on AIX: `/var/ibm/tivoli/common/COD/logs/agent/message` • **Trace files** - `<TIVOLI_COMMON_DIRECTORY>/COD/logs/agent/trace`, for example on AIX: `/var/ibm/tivoli/common/COD/logs/agent/trace`

Table 61. Problems and solutions with the agent (continued)

Problem	Potential solution
Agent status is *unknown*.	The agent has the *unknown* status when there is another agent that has the same hostname, operating system, operating system version, and it is running on the same physical host. This may happen, for example, in the following situations: • virtual machine cloning - when you clone a given VM on the same node and change only the agent ID: this feature is not supported • periodical system provisioning - when your system is frequently reinstalled; what may happen is that you may have the same system with the agent reinstalled with a different agent ID. If this is the problem, you can unregister the agent from the server because that agent was already uninstalled from the system. If you do not take any action, the agent will become inactive and later on it will be cleaned up automatically by the server.
Agent status is *incomplete*.	There are four possible actions you can perform: 1. Check if Common Inventory Technology enabler has been run. To do that use the following commands: • On Windows - `VMwareService.exe --cmd "info-get guestinfo.CIT_NODE_ID"` • On UNIX - `vmware-guestd --cmd "info-get guestinfo.CIT_NODE_ID"` If it has been run, the command should not return an empty string. 2. Check if the virtual machine (VM) manager is connected. 3. Check if the Solaris agent is deployed in the global zone and if the HP agent is installed in the Integrity VM. If it is not, install it. Note that the **Vendor** and **Brand** fields in the Web UI may be empty for the agent with the *Incomplete* status because it cannot retrieve processor information. The fields will be populated only when the agent status is **OK**.
Agent status is *old inventory*.	There are two possible solutions to this problem: 1. Schedule new software scan to update the inventory. 2. Check if you scan all the shared file systems that you are supposed to. If not, designate an agent to scan a given shared file system.

Table 61. Problems and solutions with the agent (continued)

Problem	Potential solution
A problem is reported with the agent configuration file.	The agent configuration file, `tlmagent.ini` has been damaged or removed. It is possible that this has been caused by editing the file with an editor that is not UTF-8 compliant. It is also possible that invalid values have been introduced to the file when it was being edited. You can back the file up and try to correct the errors. If the problem persists, you can uninstall the agent and then redeploy it. If you do this, you must be aware that the new agent will have a different ID, so that historical information about products installed and in use on the node will be more difficult to track. If neither of these options resolves the problem, contact IBM Software Support.
The agent fails to contact the server.	Check that the server is available to other agents. Also check if the server is available in the network by pinging it. If the server is available to other agents, it might have been unavailable temporarily to the agent when the error occurred. Stop the agent by running the `tlmagent -e` command from the agent installation directory, then start the agent by running the command: `startsrc -s tlmagent` (AIX) or `tlmagent -g` (other platforms). If the agent is already running, and it still cannot connect to the server, check if the server properties in the tlmagent.ini file are set correctly. See also tlmagent command description. If the problem persists, contact IBM Software Support and report the message.

Table 61. Problems and solutions with the agent (continued)

Problem	Potential solution
For Linux390 nodes, inconsistent capacity values are shown in the Processors window on the server Web UI.	This problem is related to the inability of the agent to retrieve the capacity value from the hardware on Linux390 computers as it does on other platforms. In order to have the information about capacity available, you must specify the value when deploying an agent. This value is stored on the agent and sent to the server during each connection. If there are two agents deployed on the node, they should both have the same capacity value, as this value relates to the node as a whole. The problem occurs if different values have been specified for capacity during the deployment of the two agents. For example, if Agent 1 has capacity = 1 and Agent 2 has capacity = 2, when Agent 1 is connected, it sends the value 1, and this is eventually recorded in the server database. When Agent 2 is connected, it sends the value 2, and the server updates its database with the new value. This series of events occurs each time the agents connect, leading to inconsistent information on the Web UI. To resolve this problem, determine what the real capacity value is for the node, and redeploy the agents with correct and consistent information.
i5/OS agents are unable to communicate. The agent is active and polling and the digital certificate has been imported using the Digital Certificate Manager (DCM), but the agent cannot detect its presence and so is not able to communicate.	Check if all agent prerequisites are installed.
The following error message appears in the agent logs: `<LogText><![CDATA[ctrlCommService - Service 2-Plugin data format error (4)]]&gt;</LogText>`.	Verify that any firewalls between agent and server have been properly configured.
Wrong VM capacity is reported by agent version 7.1 installed on an ESX virtual server.	Upgrade Common Inventory Technology to version 2.5.1032 or newer.
Problems with scheduling commands on an agent running within an AIX workload partition (WPAR) that has been relocated between LPARs using the Live Application Mobility feature can be caused by the AIX Technology Level being too old.	Upgrade AIX in the logical partition to Technology Level 6100-02-03-0909 or newer.

Table 61. Problems and solutions with the agent (continued)

Problem	Potential solution
If an unexpected agent mobility can be observed after upgrading the server version 7.1 or 7.2, it might mean that an agent installed on one of the machines in your infrastructure has not managed to upload the virtual machine hierarchy before the upgrade of the server. The agent appears in the user interface as a relocated one.	Exclude the partition from processor value unit (PVU) calculations. See: Excluding partitions.
The status of WebSphere Application Server in the WebSphere agent CLI after using the servers command is *unmanaged* (it means that the agent cannot monitor the server).	Check if you have installed WebSphere Application Server version 6.1 with either fix pack 11 or 13 because the Websphere agent cannot monitor servers with versions 6.1.0.11 and 6.1.0.13. To solve this problem, install the newer version.
During the i5/OS agent uninstallation, an error message occurs with the options `C D I R`.	This problem occurs if you are trying to uninstall the agent while a software scan is running. Select `C` and try to uninstall again after a few minutes.
The following error message appears in the agent logs when it starts for the first time after installation: `<LogText>Error ( -1 ) in storage component pageFile: Input/Output in file error</LogText>`	When an agent is started for the first time after the installation, it does not have cache files. As the agent is not able to determine whether the cache has been removed or if it is corrupted, it records a message in the agent trace file and creates a new cache file. If the problem occurs again or repeats on a regular basis it may mean that the file system is corrupted or the cache has been manually deleted.

Web user interface problems

This topic explains how to solve some common problems with the Web user interface.

Table 62. Problems and solutions for the Web user interface

Problem	Potential solution
Problems displaying national language characters. The problem refers also to the situation when you want to add a user and even though it exists in the system, you get the message: *No User was found in User Registry Repository with this name*.	To display national language characters correctly, set your national language to be the preferred one in the browser. **In Internet Explorer** 1. On the **Tools** menu, click **Internet options**. 2. In the **General** tab, click the **Languages** button. 3. Click **Add** to add your preferred language. 4. Select the language from the list, and click **OK**. 5. Select this language, and click the **Move Up** button to move the language to the first position in the list. **In Mozilla Firefox** 1. On the **Tools** menu, click **Options**. 2. Click the **Content** panel. 3. In the **Languages** section, click **Choose**, and from the drop-down list select your preferred language. 4. Click **Add** and then **Move Up** to move the language to the first position in the list.

Table 62. Problems and solutions for the Web user interface (continued)

Problem	Potential solution
Problems displaying multilingual characters. The user is unable to enter some Unicode national characters as input, or characters are corrupted.	**For the embedded WebSphere Application Server:** 1. Open the `server.xml` file, located in the directory `<INSTALL_DIR>\eWAS\profiles\AppSrv01\config\cells\cell1\nodes\node1\servers\server1\`, and back it up. 2. Modify the **genericJvmArguments** parameter: genericJvmArguments="-Dclient.encoding.override=UTF-8 3. Restart the server. **For the base WebSphere:** 1. In the administrative console, click **Servers** → **Application servers** → ***server1*** → **Java and Process Management** → **Process Definition** → **Java Virtual Machine**. 2. Enter the following value in the **Generic JVM arguments** field and save the configuration.: -Dclient.encoding.override=UTF-8 3. Restart the server.

Table 62. Problems and solutions for the Web user interface (continued)

Problem	Potential solution
GB18030 extension characters are not displayed correctly in PDF reports on Windows.	To display the GB18030 character set properly: 1. Install the GB18030 Support Package for Windows on both the server and the computer from which the user interface is launched. 2. Follow the steps described in *Problems displaying multilingual characters. The user is unable to enter some Unicode national characters as input, or characters are corrupted.* 3. Back the `fontsConfig.xml` file up. If the server is installed on the embedded WebSphere Application Server included in the installation package, the file is located in the following directory: `<INSTALL_DIR>\eWAS\systemApps\isclite.ear\tad4d_admin.war\WEB-INF\platform\plugins\org.eclipse.birt.report.engine.fonts_2.2.1.v20070823\`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\platform\plugins\org.eclipse.birt.report.engine.fonts_2.2.1.v20070823\` 4. In the original version of the file from the previous step, change the following line: <mapping name="sans-serif" font-family="Helvetica"/>into: <mapping name="sans-serif" font-family="SimSun-18030"/> 5. Restart the server.
Internet Explorer version 6 or 7 displays incorrect characters, for example Â, in the information center accessed from the Web UI.	To display these characters correctly, go to http://support.microsoft.com/default.aspx/kb/928847, and follow the methods listed in the **Resolution** section.
Problems displaying full hover help texts in Mozilla Firefox 2.	To display long hover help texts, right-click the image to which a given hover help refers and click **Properties** to view the full text.

Table 62. Problems and solutions for the Web user interface (continued)

Problem	Potential solution
Problems connecting to the Web user interface by means of a browser.	The problem occurs when the browser is not enabled for Transport Layer Security (TLS) 1.0 feature. To change the browser setting to enable TLS: **In Internet Explorer** 1. On the **Tools** menu, click **Internet options**. 2. Click the **Advanced** tab. 3. Select the **Use TLS 1.0** checkbox. **In Mozilla Firefox** 1. On the **Tools** menu, click **Options**. 2. Click the **Advanced** panel. 3. In the **Encryption** tab, select the **Use TLS 1.0** checkbox.
After logging in to the Web user interface, the whole navigation bar is expanded. Additionally, when clicking a given panel, the tabs with panel names are not visible.	The problem occurs in Internet Explorer because of too high security levels. To change the security level and add the page to the trusted zone: 1. Copy the host name from the **Address** bar, for example https://my.hostname. 2. On the **Tools** menu, click **Internet options**. 3. On the **Security** tab, click the **Trusted sites** icon, and then click the **Sites** button. 4. Paste the host name into the **Add this Web site to the zone field**, and click **OK**. 5. For the changes to take effect, refresh the page or restart the browser.
The logon page does not appear when the correct address is supplied.	Verify that the Web server is running in the list of running applications. If more than one Web server is installed on the machine where the server is installed, and both are configured to use the same port, the one that started first and is using the default port might not be compatible with the embedded WebSphere Application Server. You can verify that this is the cause of the problem by including port number 9081 or 9091 (the HTTP server transport ports) in the Web page address. If this is the cause, the page will be found. You can resolve the problem temporarily by stopping the Web servers restarting the one that is compatible with WebSphere Application Server. To resolve the problem permanently, you must configure the HTTP server and WebSphere Application Server to use a different port.

Table 62. Problems and solutions for the Web user interface (continued)

Problem	Potential solution
The browser indicates that there is a problem with the format of the HTTP header.	This problem occurs when the browser setting for the languages in use contains an entry that is not a valid language for Tivoli Asset Discovery for Distributed. Check the browser settings for the languages and remove any entries in the languages list that are not true languages, for example, [pdf].
A technical error is produced by the first action after logon.	This problem occurs when the browser is not enabled for JavaScript™. Change the browser settings to enable JavaScript and try again.
Additional windows do not open automatically.	Verify that you are using a supported Web browser.
Web interface of the server logon page closes after logging on.	The normal behavior is for the logon process to open the Web interface in a child window of the browser and then to automatically close the logon page window. There are several browser utilities that intercept the opening of pop-up windows to avoid displaying annoying advertisements. The feature that blocks the opening of pop-up windows is available in Mozilla browsers by default. This feature is not currently available in Internet Explorer 6.x browsers, but it may be installed by a browser plugin, for example, the Google toolbar. The feature must be disabled by changing the browser settings or the plugin settings to allow pop-up windows to display. If this is not possible, disable or uninstall the plugin.
The dialogs in the Web interface do not have the correct look and feel and the portfolio does not respond reliably.	This problem occurs because the JavaScript interpreter is disabled for the browser you are using. Change the settings to enable the JavaScript interpreter. You might have to restart the browser.
Problems displaying a chart.	This problem can occur when the server is installed on a UNIX platform and there is no access to an X display server. You must ensure that the server has access to an X display server.
Problems displaying report pages.	This is caused by a known problem with Internet Explorer 5.5. which is resolved with Internet Explorer 6.0. Refreshing the page using the Refresh icon on the Web interface toolbar corrects this display problem.
A specific search does not find an object but a general search does.	If the object was created with multiple consecutive spaces, the value entered for the search must include exactly the same number of spaces. The GUI will display separate words with a single space. This is a limitation of HTML, but the database stores the ID exactly as it was submitted.

Table 62. Problems and solutions for the Web user interface (continued)

Problem	Potential solution
Message dialogue boxes do not appear properly when High Contrast is enabled.	This only occurs if you change the color schema while the server installer is running. Do not modify any settings while the installer is running.
Products do not appear in reports.	If the parts that comprise a product are free, the product will not appear in audit reports.
A null pointer exception occurs while using the Web user interface.	This might occur if more than one Web page is opened in tabs (for example in Firefox) or in new windows.
Problems downloading reports in PDF format.	Verify that Java 2 Security is disabled. Open the Integrated Solutions Console and navigate to **Security** → **Secure administration, applications, and infrastructure**. Ensure that the **User Java 2 security to restrict application access to local resources** checkbox is not selected. If it is selected, unselect it, save the configuration, and restart the server.
It takes a long time for the Agent or Software Catalog Versions panels to load the data.	This happens because of performance problems caused by a huge number of scan groups. To solve the problem: 1. Set the showAgentStatus parameter to **false** and restart the server. 2. Reduce the number of scan groups by deleting some of them. 3. Set the **showAgentStatus** parameter to **true**.
After the upgrade from License Metric Tool 7.1 to Tivoli Asset Discovery for Distributed 7.2 on Windows, the link **Web interface** opens with the following message: `The page cannot be found`.	The problem occurs as License Metric Tool 7.1 stores incorrect information on the port used for User Interface. This information is used to generate the UI link in the 7.2 version. To solve the problem, you need to change the port from 9988 to 8899.

Keeping up-to-date

This topic provides the information about what you should do in order to ensure the accurate work of Tivoli Asset Discovery for Distributed.

- Import the software catalog on a regular basis. For details see *Importing the software catalog* below.

  Updates of the catalog to include new products and new signatures are produced each month.
- If you are monitoring products licensed under IBM sub-capacity conditions, import the processor value units table when necessary.

  A new table is needed if you migrate licensed products to processors of a new type that was not supported when your current table was issued and if you are creating a license with an electronic entitlement that references a later version of the table.
- Schedule regular installed software scans.

  Regular scans are required to produce up-to-date information for installed software reports. For details see the "Administering" section of the infocenter.

- Apply fix packs.

  Fix packs are available from the IBM Support Web site at regular intervals, and are cumulative, each successive fix pack containing the fixes included in previous fix packs. You do not need to apply every fix pack, but if you deploy new software or hardware you should apply the latest fix pack.

Importing the software catalog

The IBM catalog is a knowledge base of product information that provides the information required by Tivoli Asset Discovery for Distributed to recognize which products are installed and in use on monitored computers.

IBM provides regular updates to the catalog and posts them on the support Web site. Following installation or upgrade, ensure that you have the most recent catalog.

1. To obtain the IBM catalog and import it into the Tivoli Asset Discovery for Distributed server database, perform these steps in the Integrated Solutions Console:
   a. In the left navigation menu expand the **Administration** group.
   b. Click **Import Software Catalog** and then, in the console page click **Update**.

      Note: You can also use the impcat command to import the catalog. For details see the *Commands* section of the Tivoli Asset Discovery for Distributed infocenter.
2. If you experience problems downloading the updates, consider downloading the catalog onto the hard drive of your computer.
   a. Open your web browser and go to http://www-01.ibm.com/software/tivoli/support/asset-management-it/.
   b. Click **Download**.
   c. Select the file for download from the list. You will find the file on the new page that opens.
   d. Download the file to a chosen folder on your hard drive.
   e. Click the **Browse** button on the Import Software Catalog administrative console page and point to the downloaded file.
   f. Click **OK** to import the file containing the IBM catalog.

Updates of the IBM catalog to include new products and new signatures are produced at regular intervals. You do not need to import every update. However, if you install new software that needs to be monitored or if you upgrade a monitored product by applying a fix pack or installing a new release, you must import a new catalog to ensure that accurate monitoring is maintained.

Importing the processor value units table

The processor value units table is required to support processor-based pricing models in which charges differ according to the type of processor on which the licensed product is installed and running. In the table, a number of units is assigned to each processor type on which this type of pricing model is available.

Regular updates of the table are made to support changes in the processor-value unit assignment and the addition of new processor types. You do not need to import every update. A new table is required in the following circumstances:

- You acquire an electronic entitlement that references a later version of the table than the version you have imported.
- You migrate a product that is licensed under processor value unit terms to a new type of processor that is not included in the table you imported.

  When a licensed product is migrated to a processor type that is not included in the currently installed processor value units table, Asset Discovery for Distributed is unable to identify the processor type.

1. To obtain the processor values table and import it into the Asset Discovery for Distributed database, complete the following steps in the Integrated Solutions Console:
   a. In the left navigation menu expand the **Administration** group.
   b. Click **Import PVU Table** and then, in the new console page click **Update**.
2. If you experience problems downloading the updates, for example because of strict security policy in your organization, consider downloading the table onto the hard drive of your computer.
   a. Open your web browser and go to .http://www-01.ibm.com/software/tivoli/support/asset-management-it/
   b. Click **Download** and then **PVU table for Tivoli Asset Discovery for Distributed**.
   c. You will find the file on the new page that opens. Download the file to a chosen folder on your hard drive.
   d. Click **Browse** button on the same administrative console page and point to the downloaded file.
   e. Click **OK** to import the file containing the value unit table.

Chapter 3. Configuring Tivoli Asset Discovery for Distributed

You need to perform some configuration tasks during and after the installation.

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.

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.

Configuring the transaction log size

After you have installed Asset Discovery for Distributed, you need to set the size of the DB2 transaction log.

The size of the transaction log is a DB2 configuration value, which should be big enough not to allow transaction log to overflow. The speed with which the transaction log becomes filled depends on the number of products in the entire infrastructure and the number of agents.

The suggested transaction log size is the following:

- for small environments (up to 50 PVU-based products and up to 10,000 agents): 400 MB, which is the default system configuration after installation

- for medium environments (up to 150 PVU-based products and up to 20,000 agents): 1 GB. You can set this by changing the value of the **LOGFILSIZ** DB2 configuration parameter to 2500
- for large environments (up to 500 PVU-based products and up to 45,000 agents): 2 GB. You can set this by changing the value of the **LOGFILSIZ** DB2 configuration parameter to 5000.

For more information on how to configure the transaction log size, visit the DB2 information center: DB2 Information Center.

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="unqualified"

 <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 63 describes the XML elements for the nodes DTD.

Table 63. 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.
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.

Table 63. Deployment element descriptions (continued)

Element	Description
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 64. 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.			
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.			

Table 64. Server parameters in the system.properties file (continued)

Parameter	Units	Default	Minimum	Maximum
	Description			
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 65. 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 66. 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 67. Administration server parameters in the configuration database.

Parameter	Units	Default	Minimum	Maximum
	Description			
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.			

Table 67. Administration server parameters in the configuration database. (continued)

Parameter	Units	Default	Minimum	Maximum
	Description			
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.			
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 68. 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.			
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.			

Table 68. Agent configuration parameters (continued)

Parameter	Units	Default	Minimum	Maximum
	Description			
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.			
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.			

Table 68. Agent configuration parameters (continued)

Parameter	Units	Default	Minimum	Maximum
	Description			
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 69. Agent configuration commands

Command	Description
setagentconf	Sets the value and, optionally, the state of the agents configuration parameter.

Table 69. Agent configuration commands (continued)

Command	Description
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,

1. Reset the **update_enabled** parameter to `hold` .
2. Restart the server.

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
```

Implementing and removing a test configuration

You can set new of values to the parameters that control the timing of agent to Tivoli Asset Discovery for Distributed communications.

The values are set for the *Sales* scan group and override values already set for individual agents by temporarily suspending the agents level settings. The configuration is prepared in advance, put on hold and then later activated.

1. Issue the following commands to define the new configuration values, put them on hold and suspend the current agent level settings.

   ```
   setagentconf -d Sales -k upload_usage_period -v 360 -s hold -h

   setagentconf -d Sales -k down_parms_period -v 360 -s hold -h
   ```

2. Issue the following command to activate the settings.

   ```
   setagentconfstate -d Sales -k update_enabled -s active

   setagentconfstate -d Sales -k down_parms_period -s active
   ```

3. To reinstate the original agent settings, issue the following commands.

   ```
   setagentconfstate -d Sales -k update_enabled -s hold

   setagentconfstate -d Sales -k down_parms_period -s hold
   ```

   These commands send the active status to all the agents in the scan group for which settings were put on hold using the **setconfkeyvalue** parameter in the setconfkeyvalue command.

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.

File	Description
<*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.
/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).
/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).

File	Description
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.
/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.

File	Description
/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.
/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.

File	Description
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

K

L

M

N

O

P

R

S

T

U

V

W

X

Printed in USA

GI11-8749-00