IBM License Metric Tool
Version 7.5

Installing IBM License Metric Tool 7.5

GC14-7637-02

IBM License Metric Tool
Version 7.5

Installing IBM License Metric Tool 7.5

GC14-7637-02

Installation Guide

This edition applies to version 7.5 fix pack 1 of IBM Tivoli Asset Discovery for Distributed (product number 5725-C68) and to all subsequent releases and modifications until otherwise indicated in new editions.

Contents

Chapter 1. Introduction

You can use IBM® License Metric Tool to maintain an up-to-date inventory of the IBM distributed software assets in your IT infrastructure, and measure the processor value units (PVU) available to and consumed by them. It also allows you to ensure compliance with IBM subcapacity licensing requirements and demonstrate good IT governance if you are using PVU-based licensed products.

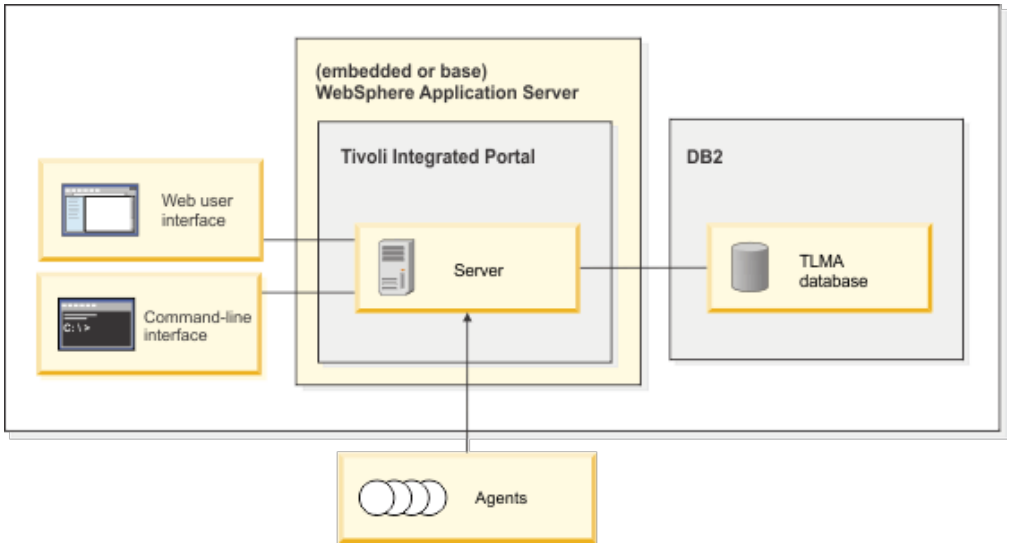
The use of License Metric Tool is required under the Passport Advantage® licensing offering, and optional for tracking full-capacity processor value unit licenses. It replaces Tivoli® License Compliance Manager for IBM software, previously required for tracking the presence of IBM software and generating required reports.

You must take ownership and administration responsibilities at the beginning of the installation process in the same way as in the case of a commercial application. It is therefore important to assign a person who will be responsible for installing, and running the product infrastructure, as well as performing all the necessary inventory and asset management tasks. For more information, see *Business roles* in the *Overview* section of the product information center.

License Metric Tool components

IBM License Metric Tool consists of an administration server, DB2® software with product database (TLMA), Tivoli Integrated Portal, WebSphere® Application Server, command-line interface, and web user interface.

License Metric Tool core components



Server components

License Metric Tool administration server
The server collects inventory data from the agents and notifies subscribed users about events that are relevant to their roles. Each

installation of License Metric Tool has a single server, which can run either on the embedded or base version of the WebSphere Application Server software.

Database for administration server

The License Metric Tool database (TLMA) runs on DB2 software. It stores the collected data, such as products installed on systems, processor value units (PVU) information, and configuration settings.

WebSphere Application Server

The embedded version of the application server is installed together with the product. The embedded application server hosts Tivoli Integrated Portal as well as License Metric Tool. For large production environments, you must install the server on the base version of WebSphere Application Server.

Tivoli Integrated Portal

Tivoli Integrated Portal is an independent component that provides a platform for the product web user interface. This interface has a single, task-based navigation panel, and users select actions based on the task that they want to complete.

Web user interface

Registered users can use the Tivoli Integrated Portal interface to perform administrative tasks, such as producing PVU capacity reports and inventory information over time.

Command-line interface

The License Metric Tool command-line interface (CLI) is one of the two user interfaces into License Metric Tool that can be used either as an efficient way to accomplish different server and agent configuration tasks by using the console.

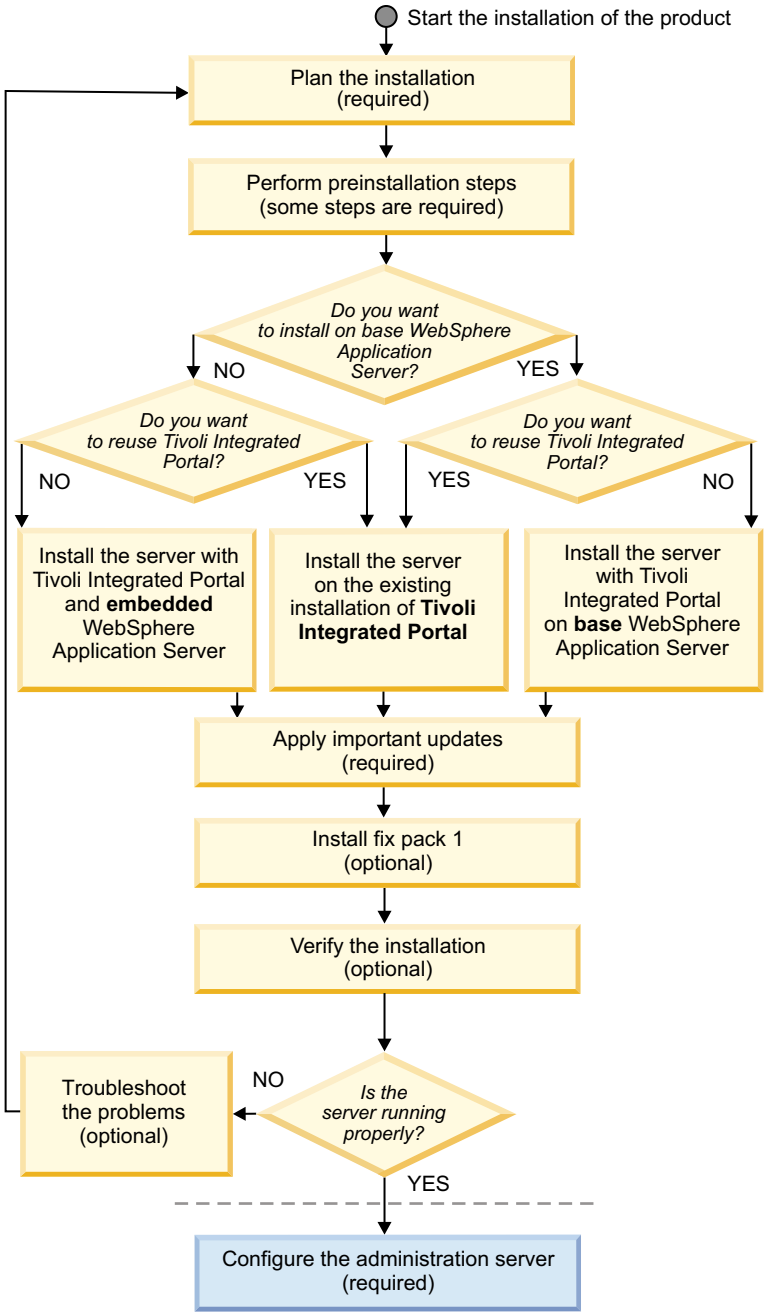
Agents

Agents are installed on each operating system that is monitored by License Metric Tool administration server. They perform hardware and software scans and forward the results to the server.

Chapter 2. Installing the administration server

Install the administration server by following one of three scenarios: either with the embedded WebSphere Application Server, on the base one, or on an existing instance of Tivoli Integrated Portal.

About this task



1. Plan the installation. Review the information in this section to learn about hardware and software requirements and other considerations.
2. Perform the necessary preinstallation steps, such as, preparing the files for installation. If you do not want to reuse an existing instance of DB2 database software, install DB2.
   Tip: Install DB2 version 9.7 as it offers the greatest performance gains.
3. Install the administration server using one of the available scenarios:
   - **scenario 1**: with Tivoli Integrated Portal and embedded WebSphere Application Server, either on a single or on two computers.
   - **scenario 2**: on an existing installation of Tivoli Integrated Portal
   - **scenario 3**: with Tivoli Integrated Portal on base WebSphere Application Server.

   Three installation methods are available:
   - Interactive installation with a wizard
   - Silent installation
   - Advanced installation
4. Required: Apply important updates, such as Tivoli Integrated Portal fix pack 2.2.0.3 and important WebSphere Application Server interim fixes.
5. Fix Pack 1 Optional: Install License Metric Tool fix pack 1.
6. Optional: Start the web user interface to verify the installation.
7. If any problems have occurred, start troubleshooting the server installation.
8. After you have installed the server, configure it.

Planning the installation of License Metric Tool server

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

About this task

- "Planning the topology"

  Depending on your needs, you can install the IBM License Metric Tool server with the **embedded** or **base** WebSphere Application Server. You can also consider installing DB2 on a separate computer.
- Scalability guidelines for IBM License Metric Tool

  Get a rough estimate on what hardware you will need for the server to handle software and hardware information discovered by agents in your environment. Specify the agent-related information on the left and check the suggested requirements on the right.
- "Supported operating systems for the server and database" on page 13

  Ensure that the computer where you are installing the IBM License Metric Tool server runs on one of the supported versions of operating systems.
- "Hardware recommendations" on page 8

  Ensure that the computer on which you are installing the IBM License Metric Tool server meets the minimal CPU, and memory requirements for the server and database elements.
- "Space requirements for the server and database" on page 10

  Check whether your computer has the required amount of disk space for server and database installation.
- "Software prerequisites for the administration server" on page 18

  Ensure that all required prerequisite software is installed on the computer where you are installing the IBM License Metric Tool server.
- "Topology and capacity planning" on page 6

  Before installing IBM License Metric Tool to monitor the installed software in your organization, you need to plan the placement of the product components.
- "Network planning" on page 20

  IBM License Metric Tool and its agents do not generate heavy data traffic for extended periods of time. However, some network planning is required.
- "Security considerations" on page 21

  There are some security issues that you must consider while installing and configuring IBM License Metric Tool.
- "Proof-of-concept installation" on page 22

  You can perform proof-of-concept installation of the product before the actual production installation. This way you can quickly set up an environment, check if it is working and if it satisfies your business needs.

Planning the topology

Depending on your needs, you can install the IBM License Metric Tool server with the **embedded** or **base** WebSphere Application Server. You can also consider installing DB2 on a separate computer.

About this task

A minimum of one administration server must be installed per License Metric Tool Region where sub-capacity programs are installed. License Metric Tool Regions are based on global continents and are defined as follows:

- Region 1: North America & South America
- Region 2: Europe & Africa
- Region 3: Asia & Australia

Procedure

1. Decide if you are going to install DB2 on the same or computer (you might also reuse it). Consider the following factors:

Table 1. Single versus two-server topology

One-server topology	Two-server topology
• Less computing power needed • Faster installation	• More processing power can be assigned to database queries. • Existing DB2 installation can be reused. • Fast network connection to the database server is needed. **Important:** The time difference between the administration server and the database server should not be grater than 300 seconds. A greater time difference might result in data loss or corruption in the server database.

2. Analyze the advantages and disadvantages of using the **embedded** versus **base** WebSphere Application Server. Determine how large your environment is and whether your infrastructure is likely to grow dramatically in the future. Consider the following factors:

Table 2. The embedded versus base WebSphere Application Server

	Embedded WebSphere Application Server	Base WebSphere Application Server
1. Number of monitored endpoints	Up to 8000	Up to 45000
2. Automatic installation of the application server	**Yes**. Embedded WebSphere Application Server installed from product installer.	**No**. Base WebSphere Application Server must be installed before installing the product
3. Automatic installation of Tivoli Integrated Portal	**Yes** (however, the existing installation can be used)	**Yes** (however, the existing installation can be used)
3. Graphical installer	**Yes**	**Yes**
4. Silent installation	**Yes**	**Yes**
5. The possibility to set up proxy servers (to connect networks)	**No**	**Yes**
6. WebSphere Application Server administration console	**No**. Advanced manual configuration/maintenance (scripted)	**Yes**. Graphical user interface for configuration/maintenance.

Note: If you choose to install IBM License Metric Tool on the embedded WebSphere Application Server, you can later upgrade it to base WebSphere Application Server. No data is lost during the upgrade.

3. Choose the appropriate installation scenario:

Table 3. Scenarios for installing the administration server

	Installation with Embedded WebSphere Application Server	**Installation on Tivoli Integrated Portal**	**Installation on base WebSphere Application Server**
1. Interactive (with a wizard)	"Installing the administration server on a single computer with embedded WebSphere Application Server" on page 31 or "Installing the administration server components in interactive mode on separate computers" on page 34	"Installing the administration server on an existing instance of Tivoli Integrated Portal" on page 41	"Installing the server in interactive mode on base WebSphere Application Server" on page 38
2. Silent	"Installing the IBM License Metric Tool server in silent mode" on page 48		

You can install the administration server in advanced mode (requires advanced administrative skills).

System growth considerations

You can plan for the growth of your infrastructure and prepare for the upgrade of the hardware or allocating more resources.

As a rule, plan hardware from the start for your target environment, not initial environment.

If you cannot predict the growth of your installation, install the administration server and the database in a virtualized operating system, for example on an AIX® logical partition (LPAR) or ESX virtual machine. This type of installation allows you to dynamically expand the environment as the requirements grow, by easily:

- adding processor cores
- allocating more memory
- changing the prioritization of system resources allocation
- migrating the installation to a computer with greater capacity.

Tip: Prepare a dedicated computer on which only the administration server and its database can be installed. This exclusive host use helps to avoid performance bottlenecks, which can happen if there are multiple server applications running on the same computer.

Topology and capacity planning

Before installing IBM License Metric Tool to monitor the installed software in your organization, you need to plan the placement of the product components.

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 scan group to which agents are assigned by default.

To find out more about scan groups, go to *Scan groups* in the *Administering* section of the Information Center.

Placement of server components

For performance reasons, it is recommended that you install the server software on a dedicated computer or on a dedicated partition (It means License Metric Tool can consume all of the available processor and memory resources allocated to a dedicated computer/partition). You can install the database on the same computer/partition as the server or on a different one. If you are installing the database on a different computer/partition than the server, you must run the installer twice on both computers/partitions.

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

- If you support fewer than 8000 agents, you can install the limited-use version of WebSphere Application Server software that is embedded with License Metric Tool.
- If you support more than 8000 agents, it is recommended that you install base WebSphere Application Server version 7 on the computer where you want to install the License Metric Tool server. One instance of WebSphere Application Server can support up to 45000 agents. You do not need an additional license for this type of WebSphere Application Server - it is covered by License Metric Tool license.

If you are installing a proxy server in your infrastructure to forward the agent-server communication, for example IBM HTTP server, it will be able to handle the same number of requests as the administration server mentioned earlier. Its performance depends on the proxy server characteristics such as processor speed, number of processors, amount of memory, and the number of running tasks and applications.

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.

Compatibility with earlier version agents

The following versions of License Metric Tool agents are able to connect to the License Metric Tool 7.5 server:

- License Metric Tool 7.5 fix pack 1

  This applies only to the environment in which administration server version 7.5 fix pack 1 is installed.
- License Metric Tool 7.5 GA
- License Metric Tool 7.2.2 GA, and Fix Pack 1
- License Metric Tool 7.2.1 GA, and Fix Pack 1
- License Metric Tool 7.2 GA, and Fix Pack 1
- License Metric Tool 7.1 GA, and Fix Pack 1
- 2.3 Fix Pack 5 or higher

Secure communications

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

Hardware recommendations

Ensure that the computer on which you are installing the IBM License Metric Tool server meets the minimal CPU, and memory requirements for the server and database elements.

Minimal CPU and memory requirements

Tip: Install DB2 version 9.7 on the latest fix pack as it offers the greatest performance gains.

The requirements are calculated for environments based on fulfilling the following assumptions:

- Approximately 50 software components in total are reported per agent on average.
- Server down time is below 5 hours per month to avoid building up significant backlog of agent data uploads.
- The underlying infrastructure, including the operating system, storage, DB2, and WebSphere server, is well-tuned.
- The system is used by maximum two concurrent users.

Table 4. Minimal CPU and memory requirements

Environment Size	Platform	Processor	Number of cores	Topology	Memory
up to **1,000** agents	Itanium	Itanium 2 1.6 GHz	1 core	Server and database on the same host	4 GB
	PowerPC®	POWER4 1.2 GHz			
	SPARC	UltraSPARC 1 GHz			
	x86 / AMD64 / Intel 64	Intel Xeon 1.5 GHz or equivalent AMD CPU			
	System z®	Type 2084 (zSeries® 990)			
up to **8,000** agents	Itanium	Itanium 2 1.6 GHz	2 cores	Server and database on the same host	4 GB
	PowerPC	POWER4 1.2 GHz			
	SPARC	UltraSPARC 1 GHz			
	x86 / AMD64 / Intel 64	Intel Xeon 1.5 GHz or equivalent AMD CPU			
	System z	Type 2084 (zSeries 990)			
up to **20,000** agents	Itanium	Itanium 2 90xx, 1.6 GHz	server: 1 core database: 2 cores	Server and database on 2 separate hosts (Distributed environment is advisable.)	server: 3 GB database: 4 GB
	PowerPC	POWER5 2.0 GHz,			
	SPARC	UltraSPARC IV 1.35 GHz			
	x86 / AMD64 / Intel 64	Intel Xeon 7xxx 2.66 GHz or equivalent AMD CPU			
	System z	Type 2094 (System z9®)			

Table 4. Minimal CPU and memory requirements (continued)

Environment Size	Platform	Processor	Number of cores	Topology	Memory
up to **45,000** agents	Itanium	Itanium 2 9000, 1.6 GHz	server: 2 cores database: 3 cores	Server and database on 2 separate hosts (Distributed environment is advisable.)	server: 3 GB database: 6 GB
	PowerPC	POWER6® 3.6 GHz			
	SPARC	SPARC64 VI 2.15 GHz			
	x86 / AMD64 / Intel 64	Intel Xeon 51xx 2.0 GHz or equivalent AMD CPU			
	System z	Type 2094 (System z9)			

Recommended CPU and memory requirements

If the assumptions for minimal CPU and memory requirements are not met or difficult to determine, apply specifications that are listed in Table 2. The calculator in scalability guidelines can also be used. To determine hardware requirements, match its output with either Table 1 (if the assumptions for minimal requirements are fulfilled) or Table 2.

Table 5. Recommended CPU and memory requirements

Environment Size	Platform	Processor	Number of cores	Topology	Memory
up to **1,000** agents	Itanium	Itanium 2 1.6 GHz	2 cores + X*	Server and database on the same host	6 GB
	PowerPC	POWER5 2.0 GHz			
	SPARC	UltraSPARC IV 1.35 GHz			
	x86 / AMD64 / Intel 64	Intel Xeon 1.5 GHz or equivalent AMD CPU			
	System z	Type 2084 (zSeries 990)			
up to **8,000** agents	Itanium	Itanium 2 90xx 1.6 GHz	server: 2 cores + X* database: 2 cores + X*	Server and database on two separate hosts (Distributed environment is advisable)	server: 3 GB database: 6 GB
	PowerPC	POWER6 3.6GHz			
	SPARC	UltraSPARC IV 1.35 GHz			
	x86 / AMD64 / Intel 64	Intel Xeon 7xxx 2.66 GHz or equivalent AMD CPU			
	System z	Type 2094 (zSeries 990)			
up to **20,000** agents	Itanium	Itanium 93xx, 1.6 GHz	server: 2 cores + X* database: 3 cores + X*	Server and database on 2 separate hosts (Distributed environment is advisable.)	server: 4 GB database: 10 GB
	PowerPC	POWER7 3.55 GHz,			
	SPARC	UltraSPARC VII 2.88 GHz			
	x86 / AMD64 / Intel 64	Intel Xeon 55xx 2.53 GHz or equivalent AMD CPU			
	System z	Type 2097 (System z10)			
up to **45,000** agents	Itanium	Itanium 93xx 1.6 GHz	server: 3 cores + X* database: 4 cores + X*	Server and database on 2 separate hosts (Distributed environment is advisable.)	server: 6 GB database: 16 GB
	PowerPC	POWER7® 3.55 GHz			
	SPARC	SPARC64 VII 2.88 GHz			
	x86 / AMD64 / Intel 64	Intel Xeon 55xx 2.53 GHz or equivalent AMD CPU			
	System z	Type 2097 (System z10®)			

X* = 1 core per each four concurrent users above two users.

Space requirements for the server and database

Check whether your computer has the required amount of disk space for server and database installation.

You can install the IBM License Metric Tool server and database on the same computer, or on two different computers. You must install the DB2 database software before you start the installation process or you can use a working installation of DB2.

Table1 shows how much space you need depending on your operating system and the components that you are installing. 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 License Metric Tool server on base WebSphere Application Server (recommended for large environments with more than 8000 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 in Table 1, remember to reserve some space for the database in the database location. When you sign a report, it is 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, the signing of the report fails. You can specify the location where the XML file is generated by editing the **reportPath** parameter in the **setserverconf** command. Additionally, in large environment, large temporary tables might be generated during aggregation or other background processes. The tables might cause that the size of DB2 increases to 20 GB. To avoid performance problems caused by the size of the database, ensure that there is sufficient amount of free disk space on the partition where the database is located.

The first installation step is the self-extraction of the installer into a temporary directory.

Windows The installer self-extracts into the `temp` directory. The directory is specified by the *TEMP* environment variable. Before the installer is extracted, the tool checks whether there is enough disk space for the installation. The required space exceeds three times the size of the installer. If there is not enough space available, the installer prompts you for a different extraction location.

UNIX The installer self-extracts into the `/tmp` directory. The tool checks whether there is enough disk space for the installation. If you specify a different location by setting the *IATEMPDIR* environment variable, the installer uses it if there is not enough space available.

Note:

1. You can specify a directory other than `/tmp` by setting the *IATEMPDIR* variable.
2. If there is not enough space in the temporary directory or the directory is not available, the installer uses the `$HOME` directory.

The requirements provided in Table 1 are for installation only.

Table 6. Space requirements for administration server components - License Metric Tool **7.5 GA**

Directory	AIX	HP-UX	Linux	Solaris	Windows
Tivoli Integrated Portal installed with **embedded** WebSphere Application Server: Linux UNIX `/opt/IBM/TIP` Windows `C:\Program files\IBM\TIP` **or** Tivoli Integrated Portal installed with **base** WebSphere Application Server: Linux UNIX `/opt/IBM/WebSphere/AppServer` Windows `C:\Program Files\IBM\WebSphere\AppServer`	0.7 - 2.3 GB	1.9 - 3.9 GB	0.7 - 2.3 GB		700 - 1000 MB
Temporary: UNIX `/var/tmp`		952 MB		952 MB	
Autonomic Deployment Engine: Linux UNIX `/usr/ibm/common/acsi` Windows `c:\Program FIles\IBM\Common\acsi`	383 - 413 MB	850 MB	383 - 413 MB		
Database instance (TLMA): Linux UNIX `/home/db2inst1` Windows `C:\Program files\IBM\sqllib`	about 760 MB				
Application installation directory: Linux UNIX `/opt/IBM/LMT` Windows `C:\Program Files\IBM\LMT`	≤ 250 MB	≤ 323 MB	≤ 250 MB		≤ 711 MB
Linux UNIX `/tmp` Windows `%TMP%`	<= 1585 MB		<= 792 MB	<= 1585 MB	≤ 170 MB
Linux UNIX `$HOME` Windows `%HOME%`	≤ 0.5 MB				≤ 20 MB
Linux UNIX `/var`	≤ 9 MB				
Tivoli Common Directory: Linux UNIX `/var/ibm/tivoli/common` Windows `C:\Program Files\IBM\tivoli\common`	2-4 MB				
Linux UNIX `/etc`	≤ 400 KB				

Table 7. Space requirements for administration server components - License Metric Tool **7.5 fix pack 1**

Directory	AIX	HP-UX	Linux	Solaris	Windows
Tivoli Integrated Portal installed with **embedded** WebSphere Application Server: Linux UNIX `/opt/IBM/TIP` Windows `C:\Program files\IBM\TIP` **or** Tivoli Integrated Portal installed with **base** WebSphere Application Server: Linux UNIX `/opt/IBM/WebSphere/AppServer` Windows `C:\Program Files\IBM\WebSphere\AppServer`	0.6 GB	1.65 GB	0.6 GB		0.6 GB
Temporary: UNIX `/var/tmp`		952 MB		952 MB	
Autonomic Deployment Engine: Linux UNIX `/usr/ibm/common/acsi` Windows `c:\Program FIles\IBM\Common\acsi`	3 MB				
Database instance (TLMA): Linux UNIX `/home/db2inst1` Windows `C:\Program files\IBM\sqllib`	2.2 GB				
Application installation directory: Linux UNIX `/opt/IBM/LMT` Windows `C:\Program Files\IBM\LMT`	0.6 GB				
Linux UNIX `/tmp` Windows `%TMP%`	1.55 GB		1.55 GB	1.55 GB	0.6 GB
Linux UNIX `$HOME` Windows `%HOME%`	2-18 MB				
Linux UNIX `/var`	4 MB				
Tivoli Common Directory: Linux UNIX `/var/ibm/tivoli/common` Windows `C:\Program Files\IBM\tivoli\common`	4-11 MB				
Linux UNIX `/etc`	≤ 400 KB				

Supported operating systems for the server and database

Ensure that the computer where you are installing the IBM License Metric Tool server runs on one of the supported versions of operating systems.

To check whether your server and database operating system is supported, click:

"AIX" | "HP-UX" | "Oracle Solaris" | "Red Hat Enterprise Linux" | "SUSE Linux Enterprise Server" on page 15 | "Windows" on page 17 | "Supported partitioning technologies - servers" on page 17

AIX

Table 8. Supported versions of AIX

Version	Required level, service packs, patches
7.1 (64-bit)	
6.1 (64-bit)	• APAR IZ37466 - to apply the fix, the AIX® 6.1 instance must be upgraded to Technology Level 3. • 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/ • APAR IZ71102 - to apply the fix, the 6.1.3.6 libc library is required
5.3 (64-bit)	

HP-UX

Table 9. Supported versions of HP-UX

Version	Required level, service packs, patches
11i v3 on Itanium (64-bit)	
11i v2 on Itanium (64-bit)	

Oracle Solaris

Table 10. Supported versions of Oracle Solaris

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

Red Hat Enterprise Linux

Restriction: The server and database can run on 64-bit system only. However, the server and database, as well as their prerequisites require 32-bit support. To install a server or database on the Red Hat Enterprise Linux 64-bit platform, you must ensure that 32-bit support is enabled. In addition to the required packages listed in the following table, you also must install the Compatibility Architecture Support or Compatibility Architecture Development Support on your system.

Important: To run IBM License Metric Tool installer in Chinese, Japanese, or Korean on Red Hat Enterprise Linux you should install one of these RPM packages:

- fonts-chinese
- fonts-japanese
- fonts-korean

Table 11. Supported versions of Red Hat Enterprise Linux

Version	Required level, service packs, patches
6 for EM64T and AMD64 (64–bit)	compat-libstdc++-33
6 for IBM Power Systems™ (64-bit)	compat-libstdc++-33 (32 and 64-bit) compat-libstdc++-295 (32 and 64-bit) Both 64-bit and 32-bit versions of the following packages: compat-db 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
6 for IBM System z(64–bit)	compat-libstdc++-295 Both 64-bit and 31-bit versions of the following packages: compat-db 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
5 for EM64T and AMD64 (64–bit)	compat-libstdc++-33 (32 and 64-bit) Both 64-bit and 32-bit versions of the following packages: compat-db libXp The following 32-bit version packages: pam cracklib-dicts cracklib glib2 libselinux

Table 11. Supported versions of Red Hat Enterprise Linux (continued)

Version	Required level, service packs, patches
5 for IBM Power Systems (64-bit)	compat-libstdc++-33 compat-libstdc++-295 Both 64-bit and 32-bit versions of the following packages: compat-db 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
5 for IBM System z (64–bit)	Update 1, compat-libstdc++-33 compat-libstdc++-295 Both 64-bit and 31-bit versions of the following packages: compat-db 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

SUSE Linux Enterprise Server

Important: To run IBM License Metric Tool installer in Chinese, Japanese, or Korean on SUSE Linux Enterprise Server you should install one of these RPM packages:

- sazanami-fonts (Japanese)
- ttf-founder-traditional (Traditional Chinese)
- baekmuk-ttf (Korean)

Table 12. Supported versions of SUSE Linux Enterprise Server

Version	Required level, service packs, patches
11 for Intel/AMD x86	
11 for EM64T and AMD64	pam-modules-32bit
11 for IBM Power Systems (64-bit)	pam-modules-32bit
11 for IBM System z (64-bit) on 64-bit hardware	pam-modules-32bit

Table 12. Supported versions of SUSE Linux Enterprise Server (continued)

Version	Required level, service packs, patches
10 for EM64T and AMD64	compat-libstdc++ (32 and 64-bit) If you plan to install DB2 9.7: Service Pack 2 glibc-2.4-31 libaio-64bit-0.3.104-14.2 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 pam-modules-32bit
10 for IBM Power Systems (64-bit)	compat-libstdc++ Service Pack 1 or later for LPAR mobility If you plan to install DB2 9.7: Service Pack 2 glibc-2.4-31 libaio-64bit-0.3.104-14.2 vacpp.rte-9.0.0-5 xlsmp.msg.rte-1.7.0-5 xlsmp.rte-1.7.0-5 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

Table 12. Supported versions of SUSE Linux Enterprise Server (continued)

Version	Required level, service packs, patches
10 for IBM System z (64-bit) on 64-bit hardware	compat-libstdc++ If you plan to install DB2 9.7: Service Pack 2 glibc-2.4-31 libaio-64bit-0.3.104-14.2 vacpp.rte-9.0.0-5 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

Windows

Table 13. Supported versions of Windows

Version	Required level, service packs, patches
Server 2008 R2 Datacenter (64-bit)	
Server 2008 R2 Standard Edition (64-bit) for Intel x86	
Server 2008 R2 Enterprise Edition (64-bit) for Intel x86	
Server 2008 Standard Edition (32 and 64-bit) for Intel x86	
Server 2008 Enterprise Edition (32 and 64-bit) for Intel x86	
Server 2003 Standard Edition (32 and 64-bit)	
Server 2003 Enterprise Edition (32 and 64-bit)	

Supported partitioning technologies - servers

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

Software prerequisites for the administration server

Ensure that all required prerequisite software is installed on the computer where you are installing the IBM License Metric Tool server.

Server installer

Table 14. Prerequisites for the administration server installer

Prerequisite	Comments
UNIX shell	To install the server on UNIX platforms, the Bourne shell (sh) must also be installed and activated. It is not necessary to run the installation from the Bourne shell. You must also install and activate the Korn shell.
Gzip compression utility	UNIX Linux It is needed for the installation process to run.
`gdiplus.dll` library	Windows This library is needed to run the License Metric Tool Launchpad.
• **Mozilla Firefox 3.6** - GA • **Microsoft Internet Explorer 8**	A browser is needed for the installation Launchpad to start.

Administration server application

Table 15. Prerequisites for the administration server application

Prerequisite	Comments
IBM Tivoli Integrated Portal 2.2	It is an independent component that provides a platform for the product web user interface. If you want to use an instance of Tivoli Integrated Portal it must be version 2.2. For more information about the product, see the product information center.
Tivoli Integrated Portal fix pack: • **2.2.0.3** - GA • **2.2.0.7** - Fix Pack 1	Use the provided Patch Installer to apply the 2.2.0.3 fix pack. This fix pack is embedded in Patch Installer platform-specific file. Download Tivoli Integrated Portal fix pack 2.2.0.7 from the fix central website.
• **Mozilla Firefox 3.6** - GA • **Mozilla Firefox 10** - Fix Pack 1 • **Microsoft Internet Explorer 8**	A web browser is required to access the web user interface of the server. However, you can start the installation of License Metric Tool without the launchpad. Supported browsers on different platforms include: **Note:** • Do not turn off the JavaScript option in your browser because some of the functionalities of the web interface might not function properly. For secure connections, cookies must be enabled. • Before using Internet Explorer, turn off Enhanced Security Configuration. Otherwise, the server web user interface might not function properly. For more information, see Disabling Internet Explorer Enhanced Security Configuration in Tivoli Integrated Portal information center. • Ensure that pop-up windows are enabled in your browser. Otherwise, the web user interface might not function properly.
JDBC driver type 4	The driver is automatically installed if not already present.

Database software

Table 16. Other prerequisites for the administration server components

Prerequisite	Comments
DB2, Enterprise Server Edition server, version 9.7 • Fix Pack 6 and higher - Fix Pack 1 This version is shipped with the product. **DB2, Enterprise Server Edition server, version 9.5** • Fix Pack 3 and higher - GA • Fix Pack 10 and higher - Fix Pack 1 **DB2, Enterprise Server Edition server, version 9.1** • Fix Pack 7 and higher - GA • Fix Pack 12 and higher - Fix Pack 1	You have two options for installing the DB2 software prerequisite: • You can install it ahead of time, by using the installation media provided with License Metric Tool. • You can use an instance of DB2 that is already installed in your environment. **Tip:** Install DB2 version 9.7 as it offers the greatest performance gains. **Note:** 1. The DB2 server must be configured for remote communication. The **svcename** parameter must be set. 2. DB2 9.1 is not supported on Windows Server 2008 R2. 3. If you want to apply Fix Pack 9 or higher to DB2 version 9.1, you need to first install License Metric Tool and then apply the fix pack. Alternatively, you can upgrade DB2 to version 9.5.
UNIX shell	To install the databases on UNIX platforms, you must have the Korn shell (ksh) installed and activated. It must 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.
Gzip compression utility	UNIX Linux It is needed for the installation process to run.

Application Server

Table 17. Other prerequisites for the administration server components

Prerequisite	Comments
WebSphere Application Server version 7.0	The following versions of the application server are supported: **Embedded** It is installed with the product (not available separately). **Base** Shipped with the product. You can install the base edition by using the version 7.0 installation media that is provided with this product, or you can use an existing installation of WebSphere Application Server 7.0. For more details, see the WebSphere Application Server version 7.0 information center. See the following web page for the list of supported software for WebSphere Application Server version 7.0. Depending on whether you have a small or a large environment, there are two options for installing WebSphere software. For more information, see "Planning the topology" on page 4.
base WebSphere Application Server fix pack 7.0.0.19	Use Update Installer to apply the fix pack on the base (or Network Deployment) version of WebSphere Application Server before installing the administration server. You can copy both platform-specific files: • Fix pack 19 for WebSphere Application Server V7.0 (file name: *partnumber*.pak) • SDK fix pack 19 for WebSphere Application Server (file name: *partnumber*.pak) from the product DVD or download it from the Passport Advantage website.

Table 17. Other prerequisites for the administration server components (continued)

Prerequisite	Comments
Global Security Toolkit interim fix	Use the provided Patch Installer to install the fix on embedded or base WebSphere Application Server: • `7.0.0.0-WS-WASJavaSDK-`*`platform`*`-IFPM47413.pak` - interim fix for **embedded** WebSphere Application Server • `7.0.0.0-WS-WASJavaSDK-`*`platform`*`-IFPM45367.pak` - interim fix for **base** WebSphere Application Server The fix is embedded in Patch Installer platform-specific file.
Fix Pack 1 **Critical security interim fixes**	Download the packages containing WebSphere Application Server interim fixes from the fix central web site. They are available under the product name category. The packages for embedded WebSphere Application Server: • `ILMT-TAD4D-Embeded-WAS-IFixes-7.5.0.10.zip` • `ILMT-TAD4D-Embeded-WAS-IFixes-7.5.0.10.tar.gz` The packages for base WebSphere Application Server: • `ILMT-TAD4D-WAS-IFixes-7.5.0.10.zip` • `ILMT-TAD4D-WAS-IFixes-7.5.0.10.tar.gz`
WebSphere Application Server interim fix for error 500	Use the provided Patch Installer to install the fix on embedded WebSphere Application Server. The file `7.0.0.17-WS-WASEmbeded-IFPM34374.pak` is embedded in Patch Installer platform-specific file, in the `common` directory.

Tip: To find out which installation packages you need, use the tool Specifying installation packages for IBM License Metric Tool 7.5.

Network planning

IBM License Metric Tool and its agents do not generate heavy data traffic for extended periods of time. However, some network planning is required.

A single agent does not require high bandwidth to communicate with the server. The amount of data exchanged with the License Metric Tool server can be as high as 350 kilobytes in a 24-hour timeframe. This includes the upload of software and hardware scan results.

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

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

License Metric Tool uses the following ports for data exchange between the server and its agents.

Note: The ports are default values that can be changed during installation.

Table 18. Ports used by License Metric Tool

Type	Port number	Description
Agent-server communication	9988	HTTP
	9999	HTTPS
	9977	HTTPS with client authentication

Table 18. Ports used by License Metric Tool (continued)

Type	Port number	Description
DB2	50000	Default TCP/IP port for database connection
Tivoli Integrated Portal	16310	The port for administration server web console
	16311	The port for administration server web console in secure mode. **Note:** The port is a default port for an 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.
	16312	Bootstrap port
	16313	Connector port for Simple Object Access Protocol (SOAP)
	16314	WebSphere Application Server console port
	16315	Secure port for WebSphere Application Server console
	16316	High Availability Manager communication port
	16318	InterProcess Connector (IPC) port
	16320	Object Request Broker (ORB) listener port
	16321	Secure Association Services (SAS) SSL server port
	16322	Client authentication listener port for Common Secure Interoperability protocol Version 2 (CSIV2)
	16323	Server authentication port for Common Secure Interoperability protocol Version 2 (CSIV2)
	16324	Representational State Transfer (REST) notification port

Security considerations

There are some security issues that you must consider while installing and configuring IBM License Metric Tool.

Required access privileges for the installation

In order to install the License Metric Tool server or agent, 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 with IBM Tivoli Configuration Manager.

Database user IDs

During the installation process, you must specify a password for the **tlmsrv** user ID. This user is supposed to perform DB2 administrative tasks, such as creating and dropping database elements.

Local operating system registries

The administration server uses only local operating system user registries during the installation of the administration server - *Lightweight Directory Access Protocol* is not supported.

Levels of security

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

Minimum
The agent communicates with the server computer on the nonsecure 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.

Ports

For the list of ports used by License Metric Tool, go to "Network planning" on page 20.

Security-Enhanced Linux

Security-Enhanced Linux set to enforcing mode can cause problems with the installation and use of License Metric Tool server and agents. If your operating system enables SELinux, you must either set it to permissive, or disable it completely.

Proof-of-concept installation

You can perform proof-of-concept installation of the product before the actual production installation. This way you can quickly set up an environment, check if it is working and if it satisfies your business needs.

Proof-of-concept installation has all the functions of the production version, but the database parameters are scaled down and the communication times between product components are reduced. If you use this mode of installation, you cannot install the Administration server and Administration server database on separate computers. You can launch proof-of-concept interactive installation by selecting **Test Environment** at the start of the server installation wizard as well as silently by setting **RSP_SETUP_TYPE** parameter to **Test**.

Note: There is a possibility to change proof-of-concept mode to production mode, however, all data gathered by the agents is always lost. To convert proof-of-concept installation into production installation, you must uninstall the database for the server component and install it again choosing **Production Environment** this time (installation with the embedded or on the base version of WebSphere Application Server).

The table includes a comparison of parameter values for test (proof-of-concept) and production environment installations.

Table 19. Proof-of-concept and production installations

Component	Configuration parameters stored in the database	Test environment	Production environment
Server	**bufferpool**	80000	80000
	system temporary tablespace	80000	80000
	upload_usage_period (minutes)	5	360
	ping_period (minutes)	2	60
	report_finalization_delay (days)	1	7
	testEnvironmentEnabled	true	false
	productInventoryBuilderPeriod (minutes)	60	300
	maxAggregateUsageAge (days)	1	2
	inventoryScanGracePeriod (hours)	1	10
Agent	**down_parms_period** (minutes)	7	360
	maxAgentInactivity (minutes)	30	10080

Installing the administration server

Install the administration server either on the embedded or base WebSphere Application Server, with a fresh instance or in an existing installation of Tivoli Integrated Portal.

Installation checklist

You can print the checklist and use it during the installation to ensure that you have completed all the necessary steps.

Table 20. The checklist for installing the administration server

Number	Installation step
1.	**Plan the installation** - ensure that the computer where you are installing the server fulfills all software and hardware requirements Before you install the server make sure that you have: • ___ planned the topology of your environment • ___ read the information about capacity planning • ___ ensured that the computer meets the minimal CPU, and memory requirements for the server and database elements and that it has enough disk space for the installation (hardware prerequisites) • ___ ensured that the computer has a supported operating system, and the necessary prerequisite software installed (software prerequisites) • ___ read the network and security planning information • ___ have decided whether you want to perform a production or proof-of-concept (test) installation first.
2.	**Perform preinstallation steps:** • ___ Prepare installation images (see also: Required software packages) • ___ Change SELinux settings • ___ Install DB2 (if you do not have a supported version instance) • ___ Install WebSphere Application Server if you do not have a supported version instance(base WebSphere Application Server scenario only) • ___ Update WebSphere Application Server - apply fix pack 19 (base WebSphere Application Server scenario only)

Table 20. The checklist for installing the administration server (continued)

Number	Installation step	
3.	**Method 1: Install the administration server interactively** - choose one of the following scenarios: Scenario 1: ___ Install the server interactively on a single computer with **embedded** WebSphere Application Server Scenario 2: ___ Install the server interactively on **base** WebSphere Application Server Scenario 3: ___ Install the server interactively on an existing instance of **Tivoli Integrated Portal** ___ You might also want to install the server interactively in **advanced mode** (advanced administrative skills are required)	**Method 2: Install the administration server in silent mode** 1. ___ Edit server installation response file 2. ___ Install the server in silent mode ___ You might also want to Install the administration server silently in **advanced mode** (advanced administrative skills are required)
4.	___ Apply important fix packs and interim fixes such as Tivoli Integrated Portal fix pack 2.2.0.3 and important WebSphere Application Server interim fixes.	
5.	___ Fix Pack 1 Install License Metric Tool 7.5 fix pack 1.	
6.	___ Verify the installation: check the log files and start the web user interface	
7.	___ Configure License Metric Tool	

Preinstallation steps

Perform some important steps before you begin the installation of the administration server.

About this task

1. "Preparing installation images" on page 25

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

   After you extract the server installer file on a given platform, a directory structure is created with various installer files.
2. "Synchronizing clocks on computers on which the administration server and database are to be installed" on page 28

   If you have decided to install the server and the database on separate computers, ensure that the time difference between the two computers is not grater than 300 seconds.
3. AIX "Extracting files from .zip packages on AIX" on page 28

   Use unzip to extract the IBM License Metric Tool server installer.
4. Linux "Changing SELinux settings before installing License Metric Tool on Red Hat Linux" on page 29

   Red Hat Enterprise Linux enables SELinux by default, which is incompatible with IBM License Metric Tool. To ensure proper server installation, you need to change the SELinux setting from enforcing mode to either permissive or disabled.
5. Installing DB2 software

   Install DB2 before you start installing IBM License Metric Tool. You can install it on the same or separate computer, depending on the size of your infrastructure.
6. Installing base WebSphere Application Server (scenario 2 or 3 only)

7. Updating base WebSphere Application Server with fix pack 19 (scenario 2 or 3 only)

Preparing installation images

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

About this task

There are two forms of installation media:

- Product disks
- The IBM Passport Advantage website. Licensed customers can download installation images for each of the DVDs.

If you are using downloaded installation images, perform the following steps to create the directory structure for a central installation image repository.

Procedure

1. Download the software from Passport Advantage. To obtain the list of the needed packages, use the interactive tool on page *Specifying installation packages for License Metric Tool 7.5* in the product information center.
2. On the computer on which you are running the installer, log on to the account with the following permissions:
   - Linux UNIX root
   - Windows Administrator
3. Place all the downloaded installation images in a single directory on the computer where you are running the installer. For example:
   - Linux UNIX

     `/install_images`
   - Windows

     `C:\install_images`

   Restriction: The path to the directory in which you place the installation images cannot contain the following characters: (space) ( )
4. Extract the contents of all installation images to the directory that you have created. It is important to extract the files on the computer where you are running the installer, because the files must have the correct permissions when you extract them from the images.

Installer files extracted from compressed packages

After you extract the installer or Patch Installer file on a given platform, a directory structure is created with various files.

Files extracted from the compressed server installer package

Table 21. The most important License Metric Tool installer files

Path	Description
Windows `server\parts\CDROM_Installers\Disk1\InstData\`*`platform`*`VM\setupServers.exe` or UNIX Linux `/server/parts/CDROM_Installers/Disk1/InstData/`*`platform`*`VM/setupServers.bin`	Internal installer files

Table 21. The most important License Metric Tool installer files (continued)

Path	Description
server\parts\CDROM_Installers\Disk1\InstData\Resource1.zipserver\parts\ CDROM_Installers\Disk1\InstData\MediaId.properties	Internal installer files
server\parts\CDROM_Installers\Disk1\InstData\desc	Image description
server\installResponsePOC.txt	The response file used in test installation
server\installResponseProduction.txt	The response file used in production installation
server\upgrade.txt	Upgrade response file
UNIX Linux server/LMT-server-7.5-*operating_system-platform_number_of_bits*.sh or Windows server\LMT-server-7.5-windows-x86_*number_of_bits*.bat	The server installer file name (by platform)
tip	directory with Tivoli Integrated Portal files
UNIX Linux tools/checkVersion.sh Windows tools\checkVersion.bat	The script checks the version of WebSphere Application Server. It calls the checkVersion.jacl script.
tools\checkVersion.jacl	The JACL script that checks the version of WebSphere Application Server
tools\getarch	Internal installer helper script
license*supported_lang_directory*	The license directory contains 16 sub directories with IBM licenses in supported national languages.
license\non_ibm_license.txt	The file contains terms and conditions for separately licensed code.
license\notices.txt	The file contains notices and third party license terms and conditions.
launchpad\	The directory contains Launchpad content, and configuration files.

Files extracted from the compressed Patch Installer package

Table 22. The directory structure with Patch Installer files, fix pack and interim fixes

Path	Description
AllPatforms\Disk1\InstData	The main jar file for the Patch Installer
common\7.0.0.17-WS-WASEmbeded-IFPM34374.pak	Tivoli Integrated Portal fix pack 2.2.0.3 for an installation with **embedded** WebSphere Application Server
W32\cdimage.fixpack	Tivoli Integrated Portal fix pack 2.2.0.3 for an installation with **embedded** and **base** WebSphere Application Server
7.0.0.0-WS-WASJavaSDK-*platform*-IFPM47413.pak	Global Security Toolkit interim fix for **embedded** WebSphere Application Server
7.0.0.0-WS-WASJavaSDK-*platform*-IFPM45367.pak	Global Security Toolkit interim fix for **base** WebSphere Application Server

A summary of installation packages

To perform the installation, you need several packages that you can download from the Passport Advantage or copy from the product DVD. Some of the images may differ depending on whether you install on the embedded or base WebSphere Application Server. You will also need fix pack files which are required for bringing WebSphere Application Server to a required software level.

Table 23. Installation packages for installing on the embedded and base WebSphere Application Server

Type of image	Embedded WebSphere Application Server	Base WebSphere Application Server
Server images	License Metric Tool 7.5 platform specific server installation package. The embedded WebSphere Application Server 7.0 is packaged with the License Metric Tool 7.5 server installation package as Tivoli Integrated Portal. Patch Installer	License Metric Tool 7.5 platform specific server installation package (includes Tivoli Integrated Portal).
WebSphere Application Server images		• WebSphere Application Server 7.0 64-bit (32-bit for Linux x86 and Win32 only) • WebSphere Application Server 7.0 Supplements, which contain: – IBM HTTP Server – Web Server Plug-ins – IBM Support Assistant – Update Installer • Fix pack 19 for WebSphere Application Server 7.0 • SDK Fix pack 19 for WebSphere Application Server 7.0 Patch Installer
DB2 images	• IBM DB2 Enterprise Server Edition 9.7 64-bit (32-bit for Linux x86 and Win32 only) • IBM DB2 Enterprise Server Edition 9.7 Restricted Use Activation	
Agent images	• License Metric Tool 7.5 agent installation package (native installer, platform-dependent) • Agent installation package, collection of Software Package Blocks only for Tivoli Configuration Manager-based installation • Agent shell installation packages for all UNIX platforms • Agent shell installation package, collection of all shell installers • Common Inventory Technology Enabler • lsof 4.80	
Documentation images	• Quick Start Guide • License Metric Tool 7.5 Quick Start - this image contains complete information center.	

License Metric Tool 7.5 fix pack 1 installation packages

Download the following packages from the fix central to install License Metric Tool 7.5 fix pack 1.

- Server images
  - License Metric Tool 7.5 fix pack 1 platform-specific server installation package.
- Agent images
  - License Metric Tool 7.5 fix pack 1 agent installation package (native installer, platform-dependent)
  - Agent installation package, collection of Software Package Blocks only for Tivoli Configuration Manager-based installation
  - Agent shell installation packages for all UNIX platforms
  - Agent shell installation package, collection of all shell installers
- Tivoli Integrated Portal fix pack 2.2.0.7
- Critical security interim fixes
  - The packages for embedded WebSphere Application Server

– The packages for base WebSphere Application Server

Synchronizing clocks on computers on which the administration server and database are to be installed

If you install the server and the database on separate computers, ensure that the time difference between the two computers is not greater 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 starts in problem determination mode, and some features are not accessible.

About this task

Use a non-manual method of clock synchronization, for example Network Time Protocol. All recent UNIX and Windows systems are able to synchronize with Network Time Protocol servers. To configure time synchronization on other operating systems, see your user documentation.

Windows The following examples show how you can ensure that the clocks are synchronized on the Windows 2008, 2003 and XP (fix pack 3 level) operating systems.

Synchronizing the time on a computer in an Active Directory domain: Procedure

1. Open the Windows command-line interface - click **Start** > **All Programs** > **Accessories** > **Command Prompt**
2. Enter the following command: **w32tm /resync** and press **Enter**.

Synchronizing an internal time server with an external source server: Before you begin

The method shown here requires that both computers are connected to the Internet.

Procedure

1. Open the Windows command-line interface
2. Enter the following command: **w32tm /config /syncfromflags:manual /manualpeerlist:***time_sources* and press **Enter**.

   where

   time_sources
   is the space-separated list of IP addresses or Domain Name System (DNS) names of time sources.

   Example: `w32tm /config /syncfromflags:manual /manualpeerlist:timeserver01.mycompany.com timeserver02.mycompany.com`

Extracting files from .zip packages on AIX

If you do not have unzip installed on your AIX server, download, install and use the program to be able to extract files from the .zip packages.

Before you begin

- Download and install the **unzip** program (`unzip-`*`program_version`*`.aix_version.ppc.rpm`) available on IBM AIX Toolbox download information website.

About this task

The following License Metric Tool installers are provided in the `.zip` format on the AIX platform:

- `ILMT-server-7.5-aix-ppc64.zip`
- `ILMT-TAD4D-patchtool-7.5-aix-ppc64.zip`
- `ILMT-TAD4D-agent-7.5-spb-all.zip`

Procedure

1. Log on to the AIX server.
2. To uncompress the server installer, issue the following command: **unzip** *installer_filename* To list the contents of the compressed file, issue **unzip -l** *installer_filename*.

Changing SELinux settings before installing License Metric Tool on Red Hat Linux

Red Hat Enterprise Linux enables SELinux by default, which is incompatible with IBM License Metric Tool. 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.

Do not set the `enforcing` mode by changing the context to `textrel_shlib_t` for all the libraries used by server.

Procedure

1. Open the `/etc/selinux/config` file.
2. Change the **SELINUX** parameter to `disabled`.
3. Restart the computer.

Information regarding installing DB2

Install DB2 before you start installing IBM License Metric Tool. You can install it on the same or separate computer, depending on the size of your infrastructure.

About this task

For information how to install DB2 refer to the highest level topics in DB2 information centers:

- Installing DB2 Version 9.7

  Tip: Install DB2 version 9.7 as it offers the greatest performance gains.
- Installing DB2 Version 9.5
- Installing DB2 Version 9.1

After you have installed DB2, you need to apply the license entitlement certificate. For information about how to do that refer to the topic *Registering a DB2 product or feature license key using the db2licm command* in the following information centers:

- DB2 9.1
- DB2 9.5
- DB2 9.7

To get the `db2ese_o.lic` license file uncompress the *DB2 Enterprise Server Edition V9.7 Restricted Use Activation* package (file name `DB2_ESE_Restricted_Activation_V97.zip`) downloaded from Passport Advantage.

You can list all the DB2 products with available license information, including the product identifier by issuing the following command: **`db2licm -l.`**.

Installing WebSphere Application Server

Before you install IBM License Metric Tool server and database, base WebSphere Application Server must already be installed. If you do not have an instance of the application server in your infrastructure, you can use the installation media for the base edition of WebSphere Application Server that is bundled with License Metric Tool.

Procedure

Locate the installation media or images for WebSphere Application Server and start the setup program. For more information about the installation procedures, consult the WebSphere documentation available in the WebSphere Application Server V7.0 information center.

Updating base WebSphere Application Server

After installing base WebSphere Application Server, you must update it with fix pack 19.

Procedure

1. Stop WebSphere Application Server.
2. Copy the WebSphere Application Server fix pack 19 file from the DVD or the directory with files downloaded from Passport Advantage to the temporary directory.
3. Run the Update Installer installation file.
4. On the **Welcome panel**, read what products are supported and click **Next**.
5. Specify the path to the WebSphere installation directory, for example:
   - UNIX Linux `/opt/IBM/WebSphere/AppServer`
   - Windows `C:\Program Files\IBM\WebSphere\AppServer`
6. Select **Install maintenance package**.
7. Enter the name of the directory where you had placed the fix pack file.
8. On the **Available Maintenance Package to install** page, select the update and fix pack files and click **Next**.
9. Click **Install**.
10. On the last page, click **Finish**. The package is installed.
11. Start WebSphere Application Server.

What to do next

To find out whether the fix pack 19 is installed, check the output from:

- Linux UNIX *WAS_HOME*`/bin/versionInfo.sh -maintenancePackages`
- Windows *WAS_HOME*`\bin\versionInfo.bat -maintenancePackages`

Example:

```
/opt/IBM/WebSphere/AppServer/bin/versionInfo.sh -maintenancePackages
```

Installing in interactive mode

When performing an interactive installation, you use the installation wizard, and provide the required parameters as the installation proceeds.

About this task

1. Perform preinstallation steps

   Perform some important steps before you begin the installation of the administration server.

2. Install the administration server based on one of the following scenarios:

Scenario 1 (option A):	"Installing the administration server on a single computer with embedded WebSphere Application Server" Use the installation wizard to specify all parameters as the installation proceeds.
Scenario 1 (option B):	"Installing the administration server components in interactive mode on separate computers" on page 34 If you want to install the database on a separate computer, you must run the installer twice on each of the computers.
Scenario 2:	"Installing the server in interactive mode on base WebSphere Application Server" on page 38 This option is intended for larger environments (up to 45,000 computers on which agents are to be installed).
Scenario 3:	"Installing the administration server on an existing instance of Tivoli Integrated Portal" on page 41 Use an available installation of Tivoli Integrated Portal to deploy the administration server.

   If there are problems, proceed to "Resuming a stopped or failed License Metric Tool installation" on page 44.

3. Verify the interactive installation

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

Installing the administration server on a single computer with embedded WebSphere Application Server

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

Before you begin

- You must have the following operating system privileges:
  - UNIX Linux root
  - Windows Administrator.
- On Windows 2008 server, run the installer using context menu entry **Run as Administrator**.
- On UNIX and Linux server computers, there must be graphical interface available, and the X server must be properly configured (the *DISPLAY* variable must be set properly). Otherwise, use silent mode.

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

Tip: DB2 is a prerequisite for License Metric Tool. Before you install it, apply the DB2 license entitlement certificate. For information about how to do that see the topic Registering a DB2 product or feature license key using the db2licm command (DB2 9.7). To get the `db2ese_o.lic` license file uncompress the *DB2 Enterprise Server Edition V9.7 Restricted Use Activation* package (file name `CZL3UML.zip`) downloaded from Passport Advantage.

Procedure

1. In the directory where you extracted the installation files, run **launchpad.exe** (Windows) or **launchpad.sh** (other platforms). The Welcome page opens.
2. In the left navigation bar, click **Install or upgrade to IBM License Metric Tool**.
3. Click **Launch the server installation wizard**. A splash screen opens.

   Tip: You can also launch the installation file

   - UNIX Linux `ILMT-server-7.5-`*`your_platform`*`.sh` or
   - Windows `ILMT-server-7.5-`*`your_platform`*`.bat` (Windows)

   directly from the `DIRECTORY_WITH_INSTALLATION_FILES\server`. You do not need the web browser for this method.
4. Select the language of the installation and click **OK**. The installation wizard starts, and the welcome panel opens. Click **Next**.
5. Read carefully the terms of the license agreement, and if you accept them all, click **Next**. Otherwise click **Cancel** and quit the installation process.
6. Specify the directory where you want to install License Metric Tool.

   Note: UNIX The installation path cannot contain spaces.
   Click **Next**.
7. On the new panel, specify the mode of installation mode that you want:
   - For typical installation, select **Production Environment**.
   - For proof-of-concept installation, select **Test Environment**.

   You can compare the differences between the Production and Test installations by reading the information in the help area on this panel.

   Note: If you select Test environment, both components are installed on the same computer.
   Click **Next**.
8. If you selected **Production Environment**, choose the components that you want to install (You can install the server and database on the same computer or on different computers). If you selected **Test Environment** in the previous step, move directly to the next step.

   If you select both components or start with the database installation, you can test the connection between the server and the database. After completing the installation of both components, you will not need to restart the server. Click **Next**.
9. On the next panel, choose one of the installation scenarios:
   - the installation of License Metric Tool with a new instance of Tivoli Integrated Portal and embedded WebSphere Application Server

- the installation of License Metric Tool with a new instance of Tivoli Integrated Portal on existing WebSphere Application Server

In this case the embedded option is described. Click **Next**.

10. Specify the path to the directory where you want to install Tivoli Integrated Portal.

    Note: UNIX The installation path for Tivoli Integrated Portal cannot contain spaces.
    Click **Next**.

11. Provide the username and password (twice) for the administrator of this instance of Tivoli Integrated Portal and click **Next**.
12. On the new panel, select **Let installation wizard select all required ports automatically** if you do not want to specify the individual ports or provide the chosen port numbers manually. Click **Next**.
13. If you have decided to install the server database, you must specify:
    - Windows The location of the DB2 instance.
    - UNIX Linux The home directory of the DB2 instance owner.

    You can enter the location of DB2 manually or you can choose from the list of found DB2 instances. The drop-down list contains all local DB2 instances found, including the ones that are not supported. They are marked with a different color and you cannot select them.

    After you have clicked **Next**, the selected database will be verified and the verification results will be presented on the panel.

    Once the Checklist items are verified, you can proceed to the next panel by clicking **Next**.
14. If you have decided to install the server, you can accept or change the ports for communication with agents. The installer checks if the ports you selected are already in use. If there are any conflicts, or you duplicated the values for the ports, a message about the problem displays.

    Click **Next** to access the next panel.
15. If you have decided to install the database for the server component, you must specify the password for the **tlmsrv** user. If the user does not exist on the system, it is created during the installation. If the user exists, the previously created password and the password you provide must match. After clicking **Next**, the password is validated for correctness. Additionally, the installation wizard searches for the existing server database in the selected DB2 instance. In case the server database is found, the installer verifies whether it can be used or migrated. If the database is not found, it is created. If you have decided not to install the server database, you must specify the details of the connection to the remote server database. After clicking **Next**, the installation wizard tries to open a JDBC connection with the provided values. Additionally, if the remote database was created by different version or product or it was created in a different mode, it is reported as a warning. Click **Next** to access the next panel.
16. 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 with the approved algorithms from the Federal Information Processing Standard 140–2. This setting applies to the server that communicates with the agents.

IBM i FIPS cannot be used on System i® platforms. If your environment includes even one agent running on IBM i, FIPS cannot be turned on.

Security Level

- If you set the minimum or medium security level, agents can communicate with the server by either the secure or nonsecure port. The selection of ports depends on the security level that you define when you deploy agents.
- If you set the maximum security level, you must set the same level of security for all agents when you deploy them.

Attention: For information about how to set the level of security before installing agents, refer to the topic *Performing agent security-related tasks*.

17. Click **Next** and review the installation information. 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. Click **Install** to install the product.

    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.
    A panel that prompts for starting the configuration process appears. Click **Next**.

    Note: If you do not click **Next** within 30 seconds, the action of moving to the next step is triggered automatically.
18. When the installation completes, click **Done** to exit the wizard.

What to do next

After both the server and database are installed, install Tivoli Integrated Portal fix pack 2.2.0.3 and important WebSphere Application Server fixes.

Installing the administration server components in interactive mode on separate computers

If you want to install the database on a separate computer, you must run the installer twice on each of the computers.

Before you begin

- You must have these operating system privileges:
  - UNIX Linux root
  - Windows Administrator
- On Windows 2008 server, run the installer using menu entry **Run as Administrator**.
- On UNIX and Linux server computers, there must be a graphical interface available, and the DISPLAY variable for the X server must be set correctly. Otherwise, use silent mode.

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

What to do next

After both the server and database are installed, install Tivoli Integrated Portal fix pack 2.2.0.3 and important WebSphere Application Server fixes.

Installing the database component on a designated computer:

As a first step, install the database for administration server. DB2 software must be installed on the computer designated for the database.

Before you begin

Tip: DB2 is a prerequisite for License Metric Tool. Before you install it, apply the DB2 license entitlement certificate. For information about how to apply the certificate, see Registering a DB2 product or feature license key using the db2licm command (DB2 9.7). To get the `db2ese_o.lic` license file, extract the *DB2 Enterprise Server Edition V9.7 Restricted Use Activation* package that you downloaded from Passport Advantage.

About this task

Start with the database installation, then perform the installation of administration server component. In this way, you can test the connection between the server and the database during the installation of the server component. When the installation of the server component is completed, the server is not to be restarted to work. If you first install the server component and then the database, you cannot check the database connection. You must restart the server after database installation is completed.

Procedure

1. In the directory where you extracted the installation files, run **launchpad.exe** (Windows) or **launchpad.sh** (other platforms). The Welcome page opens.
2. In the left navigation bar, click **Install or upgrade to IBM License Metric Tool**.
3. Click **Launch the server installation wizard**. A splash screen opens.

   Tip: You can also launch the installation file.

   - UNIX Linux `ILMT-server-7.5-`*`your_platform`*`.sh` or
   - Windows `ILMT-server-7.5-`*`your_platform`*`.bat`

   directly from the *`DIRECTORY_WITH_INSTALLATION_FILES`*`\server`. You do not need the web browser for this method.
4. Select the language of the installation and click **OK**. The installation wizard starts, and the welcome panel is displayed. Click **Next**.
5. Read the terms of the license agreement carefully. After you accept them all, click **Next**. Otherwise, click **Cancel** and quit the installation process.
6. Specify the directory in which you want to install License Metric Tool.

   Note: UNIX The installation path cannot contain spaces.
   Click **Next**.
7. On the new panel, specify your preferred installation mode:

- For typical installation, select **Production Environment**.
- For proof-of-concept installation, select **Test Environment**.

To compare the differences between the Production and Test installations, see the information in the help area on this panel.

Note: If you select Test environment, both components are installed on the same computer.
In this scenario **Production Environment** is described. Click **Next**.

8. Select **Database for administration server** and click **Next**.
9. On the next panel, specify:
   - Windows DB2 installation directory
   - UNIX Linux The home directory of the DB2 instance owner.

   You can enter the location of DB2 manually or choose from the list of discovered DB2 instances. The list contains all local DB2 instances, including those instances that are not supported. They are marked with a different color and you cannot select them.

   Click **Next**.
10. The selected database is verified and the results are presented on the new panel. Once the checklist items are verified, you can proceed to the next panel by clicking **Next**.
11. Enter the password for the **tlmsrv** user, that is to be created during the installation.

    The `tlmsrv` user is stored in an encrypted form in the application server configuration files. If the user exists, the previously created password and the password you provide must match. After clicking **Next**, the password is validated for correctness. The installation wizard searches for the existing server database in the selected DB2 instance. If the server database is found, the installer verifies whether it can be used. If it is not found, it is created.
    Click **Next**.
12. On the new panel, specify the level of security:
    - If you set the **minimum** or **medium** security level, agents can communicate with the server using either the secure or the nonsecure port. The selection of the port depends on the security level that you want to enable.
    - If you set the **maximum** security level, you must set the same level of security for all agents when you deploy them.

    Attention: For information about how to set the level of security before installing agents, see Performing agent security-related tasks.
    Click **Next**.
13. On the installation summary page, check the information that is provided and confirm that there is enough space to complete the installation. If the amount of available space is close to the total size shown, clear some space before proceeding. Click **Install** to install the database.

    Important: The installation program creates some temporary files, so more disk space might be required than the total size shown on this page. Consider this extra requirement before installing. If necessary, clear additional space.
14. A panel that prompts for starting the configuration process appears. Click **Next**.

Note: If you do not click **Next** within 30 seconds, the action of moving to the next step is triggered automatically.

15. When the installation completes, click **Done** to exit the wizard.

Installing the administration server component on a separate computer:

Install the server component on a computer different from the one on which DB2 is installed. Choose this interactive installation method to install the License Metric Tool server with embedded WebSphere Application Server.

Procedure

1. Repeat the steps 1 - 4 from the previous task. A new panel opens informing you that the database is already present on the computer. Click **Next**.
2. Specify the component to be installed. In this case, select the **Administration server** option. Click **Next**.
3. On the next panel, choose one of the installation scenarios:
   - the installation of License Metric Tool with a new instance of Tivoli Integrated Portal and embedded WebSphere Application Server
   - the installation of License Metric Tool with a new instance of Tivoli Integrated Portal on existing WebSphere Application Server

   In this case the embedded option is described. Click **Next**.
4. Specify the path to the directory where you want to install Tivoli Integrated Portal.

   Note: UNIX The installation path for Tivoli Integrated Portal cannot contain spaces.
   Click **Next**.
5. Provide the username and password (twice) for the administrator of this instance of Tivoli Integrated Portal and click **Next**.
6. On the new panel, select **Let installation wizard select all required ports automatically** if you do not want to specify the individual ports or provide all the port numbers manually. Click **Next**.
7. Accept or change the ports for communication with the agents. The installer checks if the ports you have selected are already in use, and lets you know if there are any conflicts.

   Click **Next**.
8. Specify the **tlmsrv** user password used to connect to the remote server database: The remaining values are provided and are grayed.

   Host name
   The host name or IP address of the computer where you installed the administration server database.

   Port number
   The port that is used by the instance of DB2 that is hosting the administration server database on the computer where this database is installed. The default is 50,000.

   Database user
   The default is **tlmsrv**. This user ID is necessary to access the database.

   Click **Next**. The installation wizard tries to open a JDBC connection with the provided values and a checklist is displayed. The password is validated for correctness. Additionally, the installation wizard searches for the existing

server database in the selected DB2 instance. In case the server database is found, the installer verifies whether it can be used or migrated. Click **Next**.

9. 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 with the approved algorithms from the Federal Information Processing Standard 140–2. This setting applies to the server that communicates with the agents.

   IBM i FIPS cannot be used on System i platforms. If your environment includes even one agent running on IBM i, FIPS cannot be turned on.

   Security Level

   - If you set the **minimum** or **medium** security level, agents can communicate with the server by either the secure or nonsecure port. The choice of port depends on the security level that you define when you deploy agents.
   - If you set the **maximum** security level, you must set the same level of security for all agents when you deploy them.

   Attention: For information about how to set the level of security before installing agents, refer to the topic Performing agent security-related tasks.

10. Click **Next** and review the installation information displayed 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. Click **Install** to install the product.

    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.
    A panel that prompts for starting the configuration process appears. Click **Next**.

    Note: If you do not click **Next** within 30 seconds, the action of moving to the next step is triggered automatically.

11. When the installation completes, click **Finish** to exit the wizard.

Installing the server in interactive mode on base WebSphere Application Server

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

Before you begin

- You must have the following operating system privileges:
  - UNIX Linux root
  - Windows Administrator
- On Windows 2008 server, run the installer using context menu entry **Run as Administrator**.

- On UNIX and Linux server computers, there must be graphical interface available, and the X server must be properly configured (the *DISPLAY* variable must be set properly). Otherwise, use silent mode.
- If you have downloaded the installation image from Passport Advantage, ensure that you have prepared your files for installation.

Tip: DB2 is a prerequisite for License Metric Tool. Before you install it, apply the DB2 license entitlement certificate. For information about how to do that see the topic Registering a DB2 product or feature license key using the db2licm command (DB2 9.7). To get the `db2ese_o.lic` license file uncompress the *DB2 Enterprise Server Edition V9.7 Restricted Use Activation* package (part number CZL3UML, file name `CZL3UML.zip`) downloaded from Passport Advantage.

About this task

Procedure

1. In the directory where you extracted the installation files, run **launchpad.exe** (Windows) or **launchpad.sh** (other platforms). The Welcome page opens.
2. In the left navigation bar, click **Install or upgrade to IBM License Metric Tool**.
3. Click **Launch the server installation wizard**. A splash screen opens.

   Tip: You can also launch the installation file

   - UNIX Linux `ILMT-server-7.5-`*`your_platform`*`.sh` or
   - Windows `ILMT-server-7.5-`*`your_platform`*`.bat` (Windows)

   directly from the `DIRECTORY_WITH_INSTALLATION_FILES\server`. You do not need the web browser for this method.
4. Select the language of the installation and click **OK**. The installation wizard starts and the welcome panel opens. Click **Next**.
5. Read carefully the terms of the license agreement, and if you accept them all, select the appropriate radio button, and click **Next**. Otherwise click **Cancel** and quit the installation process.
6. Specify the directory where you want to install License Metric Tool.

   Note: UNIX The installation path cannot contain spaces.
   Click **Next**.
7. On the new panel, specify the mode of installation mode that you want:
   - For typical installation, select **Production Environment**.
   - For proof-of-concept installation, select **Test Environment**.

   You can compare the differences between the Production and Test installations by reading the information in the help area on this panel.

   Note: If you select Test environment, both components are installed on the same computer.
   Click **Next**.
8. If you selected **Production Environment**, choose the components that you want to install (You can install the server and database on the same computer or on different computers). If you selected **Test Environment** in the previous step, move directly to the next step.

If you select both components or start with the database installation, you can test the connection between the server and the database. After completing the installation of both components, you will not need to restart the server.

Tip: If you first install the server and then the database, you will need to restart the server.
Click **Next**.

9. On the next panel choose one of the installation scenarios:
   - installation of License Metric Tool with a new instance of Tivoli Integrated Portal and embedded WebSphere Application Server
   - installation of License Metric Tool with a new instance of Tivoli Integrated Portal on existing base WebSphere Application Server

   In this case the installing on base WebSphere Application Server option is described. Click **Next**.
10. Specify the directory where WebSphere Application Server is installed. Click **Next**.
11. Provide the username and password (twice) for the administrator of this instance of Tivoli Integrated Portal and click **Next**.
12. On the new panel select **Let installation wizard select all required ports automatically** if you do not want to specify the individual ports or provide all the port numbers manually. Click **Next**.
13. Specify:
    - Windows The location of the DB2 instance.
    - UNIX Linux The home directory of the DB2 instance owner.

    You can enter the location of DB2 manually or you can choose from the list of found DB2 instances. The drop-down list contains all local DB2 instances found, including the ones that are not supported. They are marked with a different color and you cannot select them.

    After you have clicked **Next**, the selected database will be verified and the verification results will be presented on the panel.

    Once the Checklist items are verified, you can proceed to the next panel by clicking **Next**.
14. If you have decided to install the server, you can accept or change the ports for communication with agents. The installer checks if the ports you selected are already in use. If there are any conflicts, or you duplicated the values for the ports, a message about the problem displays.

    Click **Next** to access the next panel.
15. If you have decided to install the database for the server component, you must specify the password for the **tlmsrv** user. If the user does not exist on the system, it will be created during the installation. If the user already exists, the previously created password and the password you provide must match. After clicking **Next**, the password is validated for correctness. Additionally, the installation wizard searches for the existing server database in the selected DB2 instance. In case the server database is found, the installer verifies whether it can be used or migrated. If the database is not found, it is created. If you have decided not to install the server database, you must specify the details of the connection to the remote server database. After clicking **Next**, the installation wizard tries to open a JDBC connection with the provided values. Additionally, if the remote database was created by different version or product or it was created in a different mode, it is reported as a warning. Click **Next** to access the next panel.

16. 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 with the approved algorithms from the Federal Information Processing Standard 140–2. This setting applies to the server that communicates with the agents.

IBM i FIPS cannot be used on System i platforms. If your environment includes even one agent running on IBM i, FIPS cannot be turned on.

Security Level

- If you set the minimum or medium security level, agents can communicate with the server by either the secure or nonsecure port, depending on the security level that you define when you deploy agents.
- If you set the maximum security level, you must set the same level of security for all agents when you deploy them.

Attention: For information about how to set the level of security before installing agents, refer to the topic Performing agent security-related tasks.

17. Click **Next** and review the installation information. 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. Click **Install** to install the product.

    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.

18. When the installation completes, click **Finish** to exit the wizard.

What to do next

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, install Tivoli Integrated Portal fix pack 2.2.0.3 and important WebSphere Application Server fixes.

Installing the administration server on an existing instance of Tivoli Integrated Portal

Use an available installation of Tivoli Integrated Portal to deploy the administration server.

Before you begin

- You must have the following operating system privileges:
  - UNIX Linux root
  - Windows Administrator
- On Windows 2008 server, run the installer using context menu entry **Run as Administrator**.

- On UNIX and Linux server computers, there must be a graphical interface available, and the DISPLAY variable for the X server must be set correctly. Otherwise, use silent mode.
- If you downloaded the installation image from Passport Advantage, ensure that you have prepared your files for installation.

Tip: DB2 is a prerequisite for License Metric Tool. Before you install it, apply the DB2 license entitlement certificate. For information about how to do that see the topic Registering a DB2 product or feature license key using the db2licm command (DB2 9.7). To get the `db2ese_o.lic` license file uncompress the *DB2 Enterprise Server Edition V9.7 Restricted Use Activation* package downloaded from Passport Advantage.

About this task

Procedure

1. In the directory where you extracted the installation files, run **launchpad.exe** (Windows) or **launchpad.sh** (other platforms). The Welcome page opens.
2. In the left navigation bar, click **Install or upgrade to IBM License Metric Tool**.
3. Click **Launch the server installation wizard**. A splash screen opens.

   Tip: You can also launch the installation file

   - UNIX Linux `ILMT-server-7.5-`*`your_platform`*`.sh` or
   - Windows `ILMT-server-7.5-`*`your_platform`*`.bat` (Windows)

   directly from the `DIRECTORY_WITH_INSTALLATION_FILES\server`. You do not need the web browser for this method.
4. Select the language of the installation and click **OK**. The installation wizard starts, and the welcome panel opens. Click **Next**.
5. Read carefully the terms of the license agreement, and if you accept them all, select the radio button, and click **Next**. Otherwise click **Cancel** and quit the installation process.
6. Specify the directory where you want to install License Metric Tool.

   Note: UNIX The installation path cannot contain spaces.
   Click **Next**.
7. On the new panel, specify the mode of installation mode that you want:
   - For typical installation, select **Production Environment**.
   - For proof-of-concept installation, select **Test Environment**.

   You can compare the differences between the Production and Test installations by reading the information in the help area on this panel.

   Note: If you select Test environment, both components are installed on the same computer.
   Click **Next**.
8. If you selected **Production Environment**, choose the components that you want to install (You can install the server and database on the same computer or on different computers). If you selected **Test Environment** in the previous step, move directly to the next step.

If you select both components or start with the database installation, you can test the connection between the server and the database. After completing the installation of both components, you will not need to restart the server. Click **Next**.

9. On the next panel, choose one of the installation scenarios:
   - the installation of License Metric Tool with a new instance of Tivoli Integrated Portal and embedded WebSphere Application Server
   - the installation of License Metric Tool with a new instance of Tivoli Integrated Portal on existing WebSphere Application Server
   - the installation of License Metric Tool **on an existing instance of Tivoli Integrated Portal**

   In this case the third option is described. Click **Next**.
10. Provide the username and password for the administrator of this instance of Tivoli Integrated Portal and click **Next**.
11. Specify:
    - Windows The location of the DB2 instance.
    - UNIX Linux The home directory of the DB2 instance owner.

    You can enter the location of DB2 manually or you can choose from the list of found DB2 instances. The drop-down list contains all local DB2 instances found, including the ones that are not supported. They are marked with a different color and you cannot select them.

    After you have clicked **Next**, the selected database will be verified and the verification results will be presented on the panel.

    Once the Checklist items are verified, the next panel opens.
12. If you have decided to install the server, you can accept or change the ports for communication with agents. The installer checks if the ports you selected are already in use. If there are any conflicts, or you duplicated the values for the ports, a message about the problem displays.

    Click **Next** to access the next panel.
13. Specify the password for the **tlmsrv** user. If the user does not exist on the system, it is created during the installation. If the user exists, the previously created password and the password you provide must match. After clicking **Next**, the password is validated for correctness. Additionally, the installation wizard searches for the existing server database in the selected DB2 instance. When the server database is found, the installer verifies whether it can be used or migrated. If the database is not found, it is created. If you have decided not to install the server database, you must specify the details of the connection to the remote server database. After clicking **Next**, the installation wizard tries to open a JDBC connection with the provided values. Additionally, if the remote database was created by different version or product or it was created in a different mode, it is reported as a warning. Click **Next** to access the next panel.
14. 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 with the approved algorithms from the Federal Information Processing Standard 140–2. This setting applies to the server that communicates with the agents.

IBM i FIPS cannot be used on System i platforms. If your environment includes even one agent running on IBM i, FIPS cannot be turned on.

Security Level

- If you set the minimum or medium security level, agents can communicate with the server by either the secure or nonsecure port. The selection of the port number depends on the security level that you define when you install agents.
- If you set the maximum security level, you must set the same level of security for all agents when you deploy them.

Attention: For information about how to set the level of security before installing agents, refer to the topic Performing agent security-related tasks.

15. Click **Next** and review the installation information. 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. Click **Install** to install the product.

    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.
    A panel that prompts for starting the configuration process appears. Click **Next**.

    Note: If you do not click **Next** within 30 seconds, the action of moving to the next step is triggered automatically.
16. When the installation completes, click **Done** to exit the wizard.

What to do next

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

Resuming a stopped or failed License Metric Tool installation

There are three phases of server installation on embedded WebSphere Application Server: preinstallation, installation and postinstallation. If the installation fails or stops, there can be different ways to rerun it, depending on the phase or method used.

Procedure

There are different ways to rerun the installation and the solution depends on the phase during which the problem occurred.

- If an error occurs during the **preinstallation** phase, you can restart the installation - no additional actions are necessary (valid for interactive and silent mode).
- If you encounter an error during the **installation** phase, you need to remove the installation directory and restart the installation.
- If an error occurs during the **postinstallation** phase, there are two ways to recover from it:

- If you can run the installer in interactive mode, follow the instructions in Working with installation configuration steps.
- If you cannot run the installer in interactive mode, uninstall the product and install it again.

Tip: To find out the stage the installation stopped at, check the `msg_server.log` file and look for the following messages:

```
CODIN0463I Preinstallation phase has begun.
CODIN0464I Preinstallation phase has ended.
CODIN0465I Installation phase has begun.
CODIN0466I Installation phase has ended.
CODIN0467I Postinstallation phase has begun.
CODIN0468I Postinstallation phase has ended.
```

Working with installation configuration steps:

If you encounter a problem when installing the server (interactive or in silent mode, the configuration phase), you can use a built-in function to diagnose the problem. Initial configuration or postinstallation takes place after all the files are deployed into the destination directory. This function retrieves detailed information from installation logs. You can rerun a failed step interactively after you diagnosed and repaired a problem.

About this task

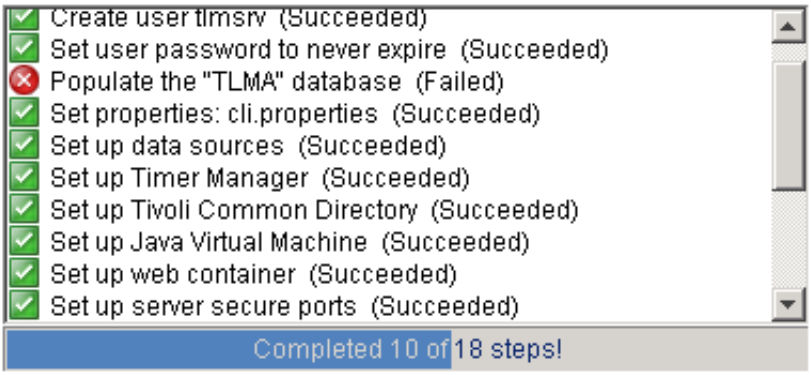
Some configuration steps depend on other steps so if one fails, the execution of the dependent step is also held. If an error occurs, the installation wizard continues running steps that do not depend on the failed one. You can see the list of prerequisites for any given step in the step properties dialog. To open the dialog, double-click the step, or select **Details** from the steps menu.

You can continue the installation and fix the problem at the end of the installation. You can also end it and resolve the problem later, at a convenient time. It is not necessary to specify any special options - it is enough to run the installation wizard again. It detects that the previous configuration attempt failed or was interrupted and starts automatically in resume mode.

If you exited the installation wizard, run it again. It automatically starts the configuration.

Procedure

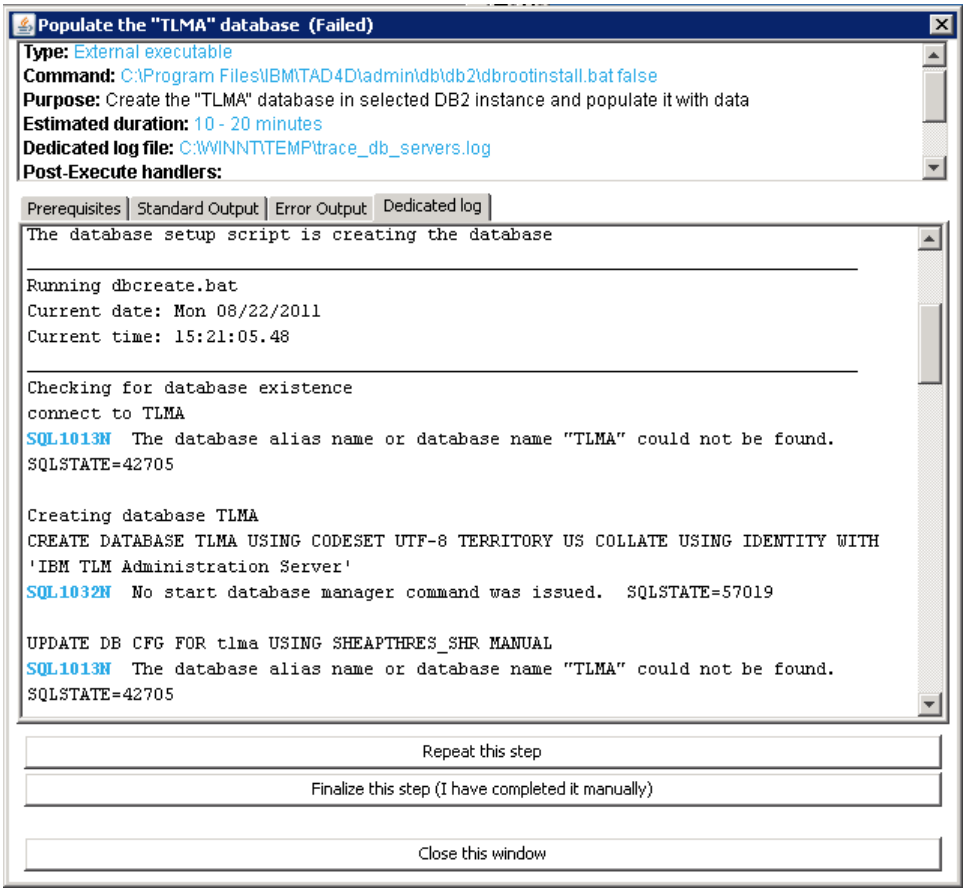
1. If you encounter a problem, double-click (or select **Properties** from the menu) the line that contains the phrase *Step name*`(Failed)`. The line is indicated by a red box.



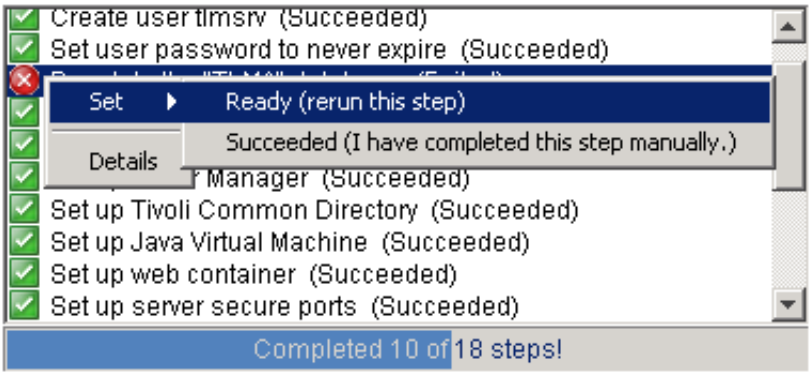
A dialog window opens.

2. Review the most important information that is displayed in the top area of the dialog window. This dialog shows (among other things) the name, and location of the dedicated log file (if applicable).
3. Review the information shown in the lower part of the dialog window to determine the root cause of the problem.

   Important: To reduce the performance load on the computer, the function that captures the dedicated log file runs with the lowest priority possible. Thus the **Dedicated log** tab does not always present the most recent and detailed information. What is more, the end of the log file might not be shown. If a failure occurs, you must check the dedicated log whose location can be found in the step description.



4. Fix the problem.
5. On the installation panel, right-click the line that shows the problem, then click **Set** > **Ready (rerun the step)**.



The installer completes the step and the remaining dependent steps.

If you have run the failed step outside the installation wizard, mark the step as completed successfully.

Note: If you cannot diagnose the problem and rerun the step manually, uninstall the product and try to install it again.

6. Click **Next**. The Postinstallation summary opens with information about installed components. Click **Done** to finish.

Installing in silent mode

When performing a silent installation, specify the parameters in the response file and start the installation from the command line.

About this task

1. "Preinstallation steps" on page 24

   Before you start the installation, prepare installation images and install DB2. If you want to install the server and the database on different computers, synchronize the date and time between those computers.
2. "Installing the IBM License Metric Tool server in silent mode" on page 48

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

   - "Server installation response files" on page 49

     Response files provide input parameters that are used when you install in silent mode.
   - "Resuming a stopped or failed License Metric Tool installation" on page 44

     There are three phases of server installation on embedded WebSphere Application Server: preinstallation, installation and postinstallation. If the installation fails or stops, there are different ways to rerun it, depending on the phase or method used.
3. "Verifying the server installation" on page 75

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

Installing the IBM License Metric Tool 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 the command line. Use this approach for unattended installation.

Before you begin

- You must have the following operating system privileges:
  - UNIX Linux root
  - Windows Administrator
- Linux UNIX Ensure that the `setupServers.bin`, and `ILMT-server-7.5-`*`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.
- Before you start the installation of the server, apply the DB2 license entitlement certificate. For information about how to do that refer to the topic Registering a DB2 product or feature license key using the db2licm command (DB2 9.7). To get the `db2ese_o.lic` license file uncompress the *DB2 Enterprise Server Edition V9.7 Restricted Use Activation* package (file name `DB2_ESE_Restricted_QS_Activation_97.zip`) downloaded from Passport Advantage.

Procedure

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 installation, edit `installResponseProduction.txt`
   - For test installation, edit `installResponsePOC.txt`

   Important: Ensure that the **`RSP_LICENSE_ACCEPTED`** parameter is uncommented and set to **true**. If you do not accept the license, the installation fails.
3. Navigate to the *`DIRECTORY_WITH_INSTALLATION_FILES`*`/server` directory. To start the installation, on the command line, run the following command:
   - Linux UNIX `ILMT-server-7.5-`*`your_platform`*`.sh –f` *`response_file_path`* `–i silent`

     Where *response_file_path* is the absolute path to the response file you are using.

     Example:

     ```
     ILMT-server-7.5-linux-ppc64.sh -f /install_images/server/
     installResponseProduction.txt -i silent
     ```
   - Windows `ILMT-server-7.5-`*`your_platform`*`.bat –f` *`response_file_path`* `–i silent`

     Where *response_file_path* is the absolute path to the response file you are using.

     Example:

     ```
     ILMT-server-7.5-windows-x86_64.bat -f c:\image\server\
     installResponseProduction.txt -i silent
     ```

What to do next

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 administration server. Then, install the agents.

Server installation response files

Response files provide input parameters that are used when you install in silent mode.

There are two installation response files:

- `installResponseProduction.txt` used for installing in production mode
- `installReponsePOC.txt` used for installing in test (proof-of-concept) mode

Both are in the `server` directory. 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 it is not against the security policy of your organization before using this installation method.

To see the input parameters that are used when you install in silent mode, click one of the following links:
| "Database parameters" on page 51 | "Server parameters" on page 51 | "Tivoli Integrated Portal parameters" on page 52

Common parameters

The following parameters are required for all installations of IBM License Metric Tool, regardless of whether you are installing the server, the database or both.

Table 24. Common response file parameters

Parameter	Parameter key name	Default
	Description	
License agreement acceptance	**RSP_LICENSE_ACCEPTED**	`true`
	Delete the hash that flags this statement as a comment. The installation fails if you do not explicitly agree with the license agreement by changing this statement from comment status.	
Installation location	**RSP_TLM_ROOT**	• Windows RSP_TLM_ROOT=C:\\Program Files\\IBM\\LMT • Linux UNIX RSP_TLM_ROOT=/opt/IBM/LMT
	Specify an empty directory where the selected elements are to be installed. If the directory does not exist, it is created. **Note:** UNIX The installation path cannot contain spaces.	

Table 24. Common response file parameters (continued)

Parameter	Parameter key name	Default
	Description	
Installation type	**RSP_SETUP_TYPE**	Production
	Specify the type of installation to be done. Possible values are: **Test** Install the server in test (proof-of-concept) mode to check whether License Metric Tool is working, and if it satisfies your business needs. **Production** Install the selected administration server components in production mode.	
Setup: administration server component selection	**RSP_ADMIN_COMPONENT**	true
	Specify whether the License Metric Tool server element is to be installed. Possible values are: **true** The server is to be installed on this computer. **false** The server is not to be installed on this computer. **Note:** This parameter is ignored during the proof-of-concept installation.	
Setup: administration database component selection	**RSP_ADMINDB_COMPONENT**	true
	Specify whether the database element is to be installed. Possible values are: **true** The database is to be installed on this computer. **false** The database is not to be installed on this computer. **Note:** This parameter is ignored during the proof-of-concept installation.	
Base configuration: **tlmsrv** user password	**RSP_TLM_TLMSRV_PASSWD**	
	Specify the password to be used to authenticate the access to the database by server processes. The password is assigned to a user with ID **tlmsrv**. This user 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 the 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 is being created. If you do not set this parameter, the installation fails. **Note:** Passwords entered in this file are not encrypted. It might be a security violation in your organization.	
Base configuration: ports used by administration server	**RSP_TLM_MIN_SEC_PORT**	9988
	The port used for minimum security level communications.	
	RSP_TLM_MED_SEC_PORT	9999
	The port used for medium security level communications (HTTPS server authentication).	
	RSP_TLM_MAX_SEC_PORT	9977
	The port used for maximum security level communications (HTTPS server and agent authentication). **Note:** If any of the selected ports is already used by a different application, the installation fails. To continue the installation and resolve the problem later, uncomment the following parameter: • **RSP_DISABLE_COMMUNICATION_WARNINGS=true**	

Database parameters

The following parameters are necessary only if you are installing the database (with or without the administration server) on the computer where silent installation is executed.

Table 25. Database parameters for silent installation

Parameter	Parameter key name	Default
	Description	
IBM DB2 database server	**RSP_TLM_DB_PATH**	
	Specify where the DB2 database server is located. If you do not set this parameter, the installer uses the DB2 instance installed on the computer. If the installer detects more than one instance of DB2 on the computer, the installation fails.	
Agent to server security level	**RSP_TLM_A2R_SEC_LEVEL**	`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 insecure 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, if 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.	

Server parameters

The following parameters are necessary only if you are installing the administration server (with or without database) on the computer where silent installation is executed.

Table 26. Parameters for silent installation of the License Metric Tool server

Parameter	Parameter key name	Default
	Description	
Administration server: remote administration database: address	**RSP_TLM_DB_HOST**	`localhost`
	Supply the host name or the IP address where the administration server database is to be installed. If you want the database to be installed on the same computer as the server, set this parameter to `localhost`. **Note:** This parameter is ignored during the proof-of-concept installation.	
Administration database port number	**RSP_TLM_DB_PORT**	`50000`
	Specify the port number used to connect to the administration server database. **Note:** This parameter is ignored during the proof-of-concept installation.	
Database connection validation	**RSP_DISABLE_DB_CONNECTION_TEST**	`false`
	It is the flag for disabling database connection test. Specify this parameter if you want to skip the validation of connection to the database.	

Table 26. Parameters for silent installation of the License Metric Tool server (continued)

Parameter	Parameter key name	Default
	Description	
Setup: Use FIPS 140-2 cryptography	**RSP_TLM_SERVER_FIPS_ENABLED**	`false`
	Specify whether encryption algorithms approved by FIPS are to be used. Possible values are: **true** FIPS 140-2 approved cryptographic algorithms are used. **false** Default algorithms are used.	

Tivoli Integrated Portal parameters

The following parameters are required for the installation of Tivoli Integrated Portal framework.

Table 27. Tivoli Integrated Portal response file parameters

Parameter	Parameter key name	Default
	Description	
Installation of Tivoli Integrated Portal in WebSphere Application Server home directory	**RSP_INSTALL_TIP_INTO_WAS_HOME**	`false`
	When set to true, it indicates your intent to install into an existing WebSphere Application Server base installation. A setting of false indicates your intent to: • install Tivoli Integrated Portal with an embedded WebSphere Application Server • reuse the existing instance of Tivoli Integrated Portal .	
Home directory for Tivoli Integrated Portal	**RSP_TIP_HOME**	`C:\\IBM\\Tivoli\\TIP`
	Set this parameter to: • indicate where you want to install Tivoli Integrated Portal with an embedded WebSphere Application Server • provide the location of an existing Tivoli Integrated Portal • provide the location of an existing instance of base WebSphere Application Server. If you are installing into an existing base WebSphere Application Server provide the base WebSphere Application Server location (also called the WAS_HOME). When you are installing with an embedded WebSphere Application Server, the default directory is: • `C:\\IBM\\Tivoli\\TIP` The \ backslash is seen as an escape character. Use \\ two backslashes when defining the path. • `/opt/IBM/tivoli/tip` **Note:** UNIX The installation path cannot contain spaces.	
Auto-assignment of ports for Tivoli Integrated Portal	**RSP_TIP_AUTO_SELECT_PORTS**	`true`
	The value `false` turns of the automatic assignment of ports to Tivoli Integrated Portal. If so, all the ports must be defined in the response file. Auto assignment begins with port 6310. The ports which were defined in the response file do not get the numbers assigned.	
Tivoli Integrated Portal administrator name	**RSP_TIP_ADMIN_NAME**	`tipadmin`
	Tivoli Integrated Portal administrator name	

Table 27. Tivoli Integrated Portal response file parameters (continued)

Parameter	Parameter key name	Default
	Description	
Tivoli Integrated Portal administrator password	**RSP_TIP_ADMIN_PASSWD**	tippass
	Tivoli Integrated Portal administrator password	
The port for administration server web console	**RSP_TIP_WC_PORT**	16310
	The port used by the administration server console.	
Secure port for administration server web console	**RSP_TIP_WC_SECURE_PORT**	16311
	The port used by the administration server console in secure mode.	
WebSphere Application Server-related parameters		
Bootstrap port	**RSP_TIP_BOOTSRAP_PORT** The TCP/IP port on which the name service listens. This port is also the Remote Method Invocation (RMI) connector port.	16312
Connector port for Simple Object Access Protocol (SOAP)	**RSP_TIP_SOAP_CONNECTOR_PORT** The TCP/IP port that your server uses for SOAP.	16313
WebSphere Application Server console port	**RSP_TIP_WC_ADMIN_PORT** This port is used to access the administrative application of WebSphere Application Server.	16314
Secure port for WebSphere Application Server console	**RSP_TIP_WC_ADMIN_SECURE_PORT** If security is enabled, this is the secure port used to access the administrative application of WebSphere Application Server.	16315
High Availability Manager communication port	**RSP_TIP_DCS_UNICAST_PORT**	16316
InterProcess Connector (IPC) port	**RSP_TIP_IPC_CONNECTOR_PORT** Port used for management communications between WebSphere Application Server processes	16318
Object Request Broker (ORB) listener port	**RSP_TIP_ORB_LISTENER_PORT** Port used for communications using the Java™ Remote Method Invocation interface over the Internet Inter-ORB Protocol (RMI/IIOP)	16320
Secure Association Services (SAS) SSL server port	**RSP_TIP_SAS_SSL_SERVERAUTH_PORT** The TCP/IP port on which the Secure Association Services (SAS) listen for inbound authentication requests.	16321
Client authentication listener port for Common Secure Interoperability protocol Version 2 (CSIV2)	**RSP_TIP_CSIV2_SSL_MUTUALAUTH_PORT** The TCP/IP port on which the Common Secure Interoperability Version 2 (CSIV2) Service listens for inbound client authentication requests.	16322

Table 27. Tivoli Integrated Portal response file parameters (continued)

Parameter	Parameter key name	Default
	Description	
Server authentication port for Common Secure Interoperability protocol Version 2 (CSIV2)	**RSP_TIP_CSIV2_SSL_SERVERAUTH_PORT** The TCP/IP port on which the Common Secure Interoperability Version 2 (CSIV2) Service listens for inbound server authentication requests.	16323
Representational State Transfer (REST) notification port	**RSP_TIP_REST_NOTIFICATION_PORT**	16324

Installing the administration server in advanced mode

If you want to fine-tune your environment, you can install the administration server in advanced mode. This mode requires high administrative skills.

Before you begin

- You must have the following operating system privileges:
  - UNIX Linux root
  - Windows Administrator
- On Windows 2008 server, run the installer using context menu entry **Run as Administrator**.
- If you have downloaded the installation image from Passport Advantage, ensure that you have prepared your files for installation.
- On UNIX and Linux server computers, there must be graphical interface available, and the X server must be properly configured (the *DISPLAY* variable must be set properly). Otherwise, install the administration server manually in advanced mode.
- Certain configuration actions have pre- and postexecute tasks. In case the action is performed outside of the installation wizard the task must be executed before or after a given configuration action. When the task is executed with the assistance of the installation wizard, pre- and postexecute tasks are performed automatically.

Tip: DB2 is a prerequisite for License Metric Tool. Before you install it, apply the DB2 license entitlement certificate. For information about how to do that see the topic Registering a DB2 product or feature license key the db2licm command (DB2 9.7). To get the `db2ese_o.lic` license file uncompress the *DB2 Enterprise Server Edition V9.7 Restricted Use Activation* package (file name `DB2_ESE_Restricted_Activation_V97.zip`) downloaded from Passport Advantage.

About this task

Most of the configuration tasks are done with JACL scripts. Each JACL script takes the `setupWAS.properties` file as a parameter. The `setupWAS.properties` file is filled out automatically with values provided during preinstallation with one exception: **`dbPassword`**. This value is required for the `setupDataSources.jacl` script.

Important: Ensure that you provide the value for **`dbPassword`** before executing the `setupDataSources.jacl` script.

Table 28. Configuration tasks and their script files

Number	Task	Configuration script
1.	Set the user password to never expire	Windows only `PwdNoExpire.exe`
2.	Populate the TLMA database	• UNIX Linux `dbrootinstall.sh` • Windows `dbrootinstall.bat`
3.	Set up data sources	`setupDataSources.jacl`
4.	Set up Timer Manager	`setupTimerManager.jacl`
5.	Set up Tivoli Common Directory	`setupTivoliCommonDir.jacl`
6.	Set up Java Virtual Machine	`setupJVM.jacl`
7.	Set up web container	`setupWebContainer.jacl`
8.	Set up server secure ports	`setupServerSecurePorts.jacl`
9.	Deploy administration server application on Tivoli Integrated Portal	`installAdmin.jacl`
10.	Deploy Message Handler application on Tivoli Integrated Portal	`installMessageHandler.jacl`
11.	Set up user roles	• UNIX Linux `setupTIP.sh` • Windows `setupTIP.bat`
12.	Set file permissions	• UNIX Linux `set_perms.sh` • Windows `set_perms.bat`

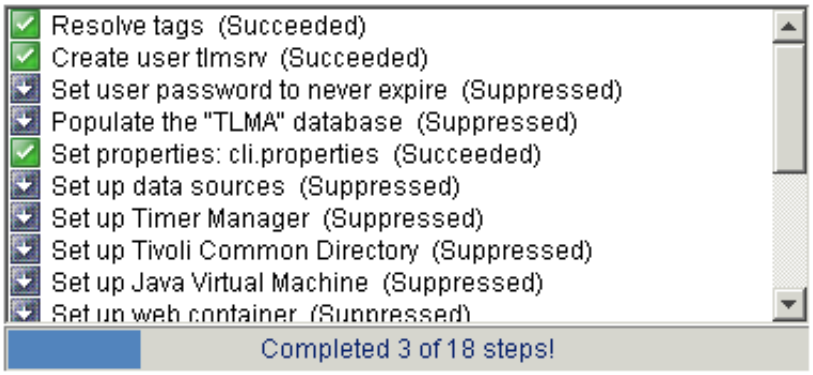
Option 1: Installing the server interactively in advanced mode

Use the installation wizard to start the advanced installation

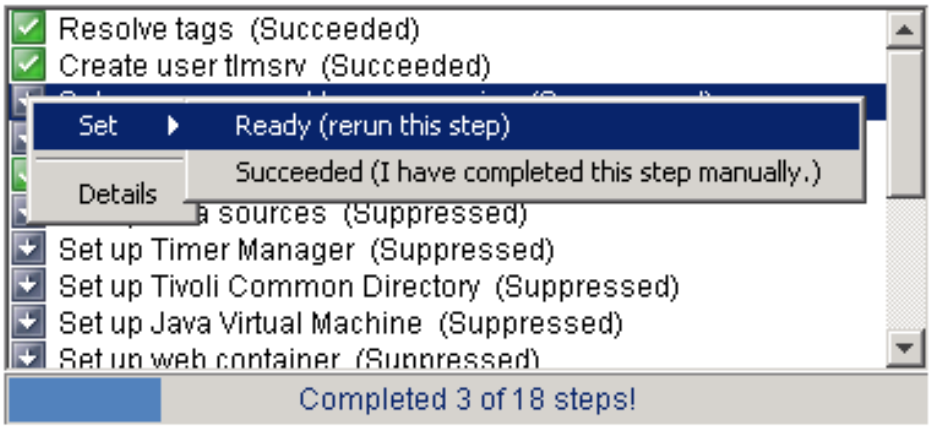
Procedure

1. Enable the suppressing of administration server configuration. Start the command-line interface and enter the following command:
   - UNIX `export RSP_SUPPRESS_CONFIG=true`
   - Windows `set RSP_SUPPRESS_CONFIG=true`
2. At the command-line prompt type:
   - UNIX Linux `ILMT-server-7.5-`*`your_platform`*`.sh` or
   - Windows `ILMT-server-7.5-`*`your_platform`*`.bat`

   Press **Enter**. A splash screen opens.
3. Perform steps 4- 17 listed in Installing the administration server on a single computer with embedded WebSphere Application Server. A panel with suppressed steps appears.



4. Make your changes in scripts. For the complete list of scripts, see the table Table 28 on page 55.
5. Perform configuration tasks 1 - 12 listed in table Table 28 on page 55- rerun each suppressed step by right-clicking it and selecting **Set** > **Ready (rerun this step)**.



.

6. When the confirmation panel appears, click **Finish**.

Results

You have installed the administration server interactively in advanced mode.

What to do next

After both the server and database are installed, install Tivoli Integrated Portal fix pack 2.2.0.3 and important WebSphere Application Server fixes.

Option 2: Installing the administration server silently in advanced mode

Install the administration server silently in advanced mode to tailor the product to your individual needs. This method requires advanced administrative skills.

About this task

Tip:

- If you want to install both components perform all the steps.

- If you want to install only the database, perform steps 1-5, and remove the contents of the resume directory (the last step).
- If you want to install only the server, perform steps 1-3, and execute the JACL scripts (step 7).

`WAS_home_dir` is the home directory of either the embedded or base WebSphere Application Server.

Table 29. Typical installation paths with the administration server installed on Tivoli Integrated Portal

Type of application server	WAS_home_dir
Embedded WebSphere Application Server	any directory, for example `/opt/IBM/TIP`
Base WebSphere Application Server	• UNIX `/opt/IBM/WebSphere/AppServer` • Windows `c:\Program Files\IBM\WebSphere\AppServer\`

Procedure

1. Enable the suppressing of administration server configuration. Start the command-line interface and enter the following command:
   - UNIX Linux `export RSP_SUPPRESS_CONFIG=true`
   - Windows `set RSP_SUPPRESS_CONFIG=true`
2. Perform the steps listed in Installing the administration server in silent mode. The silent installation will stop after some time and the information about entering the advanced mode will be written to the logs. Several steps have been suppressed as a result of silent installation. The steps are listed in table Table 28 on page 55.
3. Make your changes in scripts. For the list of scripts, see the table Table 28 on page 55.
4. Start the operating system command-line interface and set the user password to never expire by entering the following command:
   - UNIX Linux not applicable
   - Windows *lmt_install_dir*`\tmp\PwdNoExpire.exe tlmsrv`
5. Populate the TLMA database by running the following script:
   - UNIX Linux *product_install_dir*`/admin/db/db2/dbrootinstall.sh true`
   - Windows *product_install_dir*`\admin\db\db2\dbrootinstall.bat true`

   Example:

```
/opt/IBM/LMT/admin/db/db2/dbrootinstall.sh true
```

6. Change to the directory:
   - UNIX Linux *product_install_dir*`/admin/setup`
   - Windows *product_install_dir*`\admin\setup`

   Example:

```
cd /opt/IBM/LMT/admin/setup
```

7. Execute JACL scripts to perform configuration tasks 3 - 8, listed in table Table 28 on page 55:
   - `setupDataSources.jacl`
   - `setupTimerManager.jacl`
   - `setupTivoliCommonDir.jacl`
   - `setupJVM.jacl`
   - `setupWebContainer.jacl`
   - `setupServerSecurePorts.jacl`
   - UNIX Linux *WAS_home_dir*/profiles/TIPProfile/bin/wsadmin.sh -lang jacl -f *script_name* setupWAS.properties
   - Windows *WAS_home_dir*\profiles\TIPProfile\bin\wsadmin.bat -lang jacl -f *script_name* setupWAS.properties

   where

   script_name
   is the name of a given JACL configuration script

   setupWAS.properties
   is the name of the WebSphere Application Server configuration file. You can also edit this file prior running the commands.

   Example:

```
/opt/IBM/WebSphere/AppServer/profiles/profiles/TIPProfile/bin/wsadmin.sh -lang jacl
-f setupDataSources.jacl setupWAS.properties
```

   Note: After executing the `setupDataSources.jacl` script, you are asked to provide a valid password for the **tlmsrv** user that you have already provided in installation response file. The other option is to provide this **tlmsrv** password as password parameter in `setupWAS.properties` file.

   Tip: WebSphere Application Server repeatedly asks for the Tivoli Integrated Portal administrator name, and password. If you do not want to provide them after each command, add username and password parameters to every JACL file execution.

   Example:

```
/opt/IBM/WebSphere/AppServer/profiles/TIPProfile/bin/wsadmin.sh -username tipadmin
-password yourpassword -lang jacl -f setupTivoliCommonDir.jacl setupWAS.properties
```

8. Restart the administration server.
   a. Stop the WebSphere Application Server by entering the command:
      - UNIX Linux *WAS_home_dir*/profiles/TIPProfile/bin/stopServer.sh *server_name* -username *username* -password *password*
      - Windows *WAS_home_dir*\profiles\TIPProfile\bin\stopServer.bat *server_name* -username *username* -password *password*

      Example:

```
/opt/IBM/WebSphere/AppServer/profiles/TIPProfile/bin/stopServer.sh server1 -username
tipadmin -password abcd1234
```

b. Start the WebSphere Application Server by running the following command:

- UNIX Linux *WAS_home_dir*/profiles/TIPProfile/bin/startServer.sh *server_name*
- Windows *WAS_home_dir*\profiles\TIPProfile\bin\startServer.bat *server_name*

Example:

```
/opt/IBM/WebSphere/AppServer/profiles/TIPProfile/bin/startServer.sh server1
```

9. Install the administration server application on Tivoli Integrated Portal:
   a. Deploy the administration server application by entering the following command:
      - UNIX Linux *WAS_home_dir*/profiles/TIPProfile/bin/wsadmin.sh -lang jacl -f installAdmin.jacl setupWAS.properties
      - Windows *WAS_home_dir*\profiles\TIPProfile\bin\wsadmin.bat-lang jacl -f installAdmin.jacl setupWAS.properties

      Example:

```
/profiles/TIPProfile/bin/wsadmin.sh -lang jacl -f installAdmin.jacl
setupWAS.properties
```

   b. Remove the file tad4d_admin.war from the following directory:
      - UNIX Linux *WAS_home_dir*/installableApps/
      - Windows *WAS_home_dir*\installableApps\

      Example:

```
rm /opt/IBM/WebSphere/AppServer/installableApps/tad4d_admin.war
```

   c. Create directory stand-alone at the following location:
      - UNIX Linux *WAS_home_dir*/profiles/TIPProfile/installedApps/TIPCell/isc.ear/tad4d_admin.war/webdoc
      - Windows *WAS_home_dir*\profiles\TIPProfile\installedApps\TIPCell\isc.ear\tad4d_admin.war\webdoc

      Example:

```
mkdir /opt/IBM/WebSphere/AppServer/profiles/TIPProfile/installedApps/TIPCell/
isc.ear/tad4d_admin.war/webdoc/stand-alone
```

   d. Copy the file stdas_scanner.zip from the following directory:
      - UNIX Linux *product_installation_dir*/ears
      - Windows *product_installation_dir*\ears

      to:
      - UNIX Linux *WAS_home_dir*/profiles/TIPProfile/installedApps/TIPCell/isc.ear/tad4d_admin.war/webdoc/stand-alone
      - Windows *WAS_home_dir*\profiles\TIPProfile\installedApps\TIPCell\isc.ear\tad4d_admin.war\webdoc\stand-alone

      Example:

```
cp /opt/IBM/LMT/ears/stdas_scanner.zip /opt/IBM/WebSphere/AppServer/profiles/
TIPProfile/installedApps/TIPCell/isc.ear/tad4d_admin.war/webdoc/stand-alone
```

10. Install the Message Handler application on Tivoli Integrated Portal:
    a. Install the application by entering the following command:
       - UNIX Linux `wsadmin.sh -lang jacl -f installMessageHandler.jacl setupWAS.properties`
       - Windows `wsadmin.bat -lang jacl -f installMessageHandler.jacl setupWAS.properties`

       Example:

```
/opt/IBM/WebSphere/AppServer/profiles/profiles/TIPProfile/bin/wsadmin.sh -lang jacl
-f installMessageHandler.jacl setupWAS.properties
```

    b. Copy the directory:
       - UNIX Linux */lmt_install_dir*/IBM/LMT/ears/selfupdate
       - Windows *lmt_install_dir*\IBM\LMT\ears\selfupdate

       to:
       - UNIX Linux *WAS_home_dir*/profiles/TIPProfile/installedApps/TIPCell/LMT-TAD4D_Agent_message_handler.ear/com.ibm.license.mgmt.msghandler.web.war/webdoc/agent/selfupdate
       - Windows *WAS_home_dir*\profiles\TIPProfile\installedApps\TIPCell\LMT-TAD4D_Agent_message_handler.ear\com.ibm.license.mgmt.msghandler.web.war\webdoc\agent\selfupdate

       Example:

```
cp -R /opt/IBM/LMT/ears/selfupdate /opt/IBM/WebSphere/AppServer/profiles/TIPProfile/installedApps/TIPCell/
LMT-TAD4D_Agent_message_handler.ear/com.ibm.license.mgmt.msghandler.web.war/webdoc/agent/
```

    c. Copy the directory:
       - UNIX Linux *lmt_install_dir*/IBM/LMT/ears/selfupd
       - Windows *lmt_install_dir*\IBM\LMT\ears\selfupd

       to:
       - UNIX Linux *tip_install_dir*/TIP5/profiles/TIPProfile/installedApps/TIPCell/LMT-TAD4D_Agent_message_handler.ear/com.ibm.license.mgmt.msghandler.web.war/webdoc/agent/selfupdate
       - Windows *tip_install_dir*\TIP5\profiles\TIPProfile\installedApps\TIPCell\LMT-TAD4D_Agent_message_handler.ear\com.ibm.license.mgmt.msghandler.web.war\webdoc\agent\selfupdate

       Example:

```
cp -R /opt/IBM/LMT/ears/selfupd /opt/IBM/WebSphere/AppServer/profiles/TIPProfile/installedApps/TIPCell/
LMT-TAD4D_Agent_message_handler.ear/com.ibm.license.mgmt.msghandler.web.war/webdoc/agent/
```

11. Set up user roles by entering the following command:
    - UNIX Linux *product_install_dir*/admin/setup/setupTIP.sh *TIP_admin_name TIP_admin_password*

- Windows *product_install_dir*\admin\setup\setupTIP.bat *TIP_admin_name TIP_admin_password*

  Example:

```
/opt/IBM/TAD4D/admin/setup/setupTIP.sh tipadmin Abcd1234
```

12. Set up file permissions (applicable only on the UNIX or Linux platform):

    UNIX Linux *product_install_dir*/IBM/LMT//tmp/set_perms.sh

    Example:

```
/opt/IBM/LMT/tmp/set_perms.sh
```

13. Remove the contents of the resume folder:
    - UNIX Linux product_installation_dir/resume
    - Windows product_installation_dir\resume

    Example:

```
rm -Rf product_installation_dir/resume/*
```

Results

You have installed administration server with the advanced method.

What to do next

After both the server and database are installed, install Tivoli Integrated Portal fix pack 2.2.0.3 and important WebSphere Application Server fixes.

Applying important fix packs and interim fixes

Install Tivoli Integrated Portal fix pack 2.2.0.3 and important WebSphere Application Server interim fixes.

About this task

Important: Do not apply these fix packs and interim fixes if you are installing License Metric Tool 7.5 and applying License Metric Tool 7.5 fix pack 1. Applying License Metric Tool 7.5 fix pack 1 includes these fix packs and interim fixes.

The choice of files depends on the type of application server that is installed in your infrastructure.

Table 30. List of important fix packs and interim fixes

Importance	Embedded	Base
Required	1. Tivoli Integrated Portal fix pack 2.2.0.3	1. Tivoli Integrated Portal fix pack 2.2.0.3
Required in case of medium or maximum security level	2. Global Security Toolkit interim fix	2. Global Security Toolkit interim fix
Required in case of medium or maximum security level	3. WebSphere Application Server interim fix for error 500	not applicable

Updating Tivoli Integrated Portal and WebSphere Application Server interactively using the Patch Installer

Use the provided Patch Installer to quickly update Tivoli Integrated Portal, and WebSphere Application Server with important fix packs, and interim fixes.

Before you begin

Copy the compressed Patch Installer from one of the DVDs or from Passport Advantage to a temporary directory on the computer where the administration server is installed, and uncompress the file.

Windows To successfully uncompress the file, use an archive manager other than the one built into Windows.

Procedure

1. Change to the temporary directory where you store the uncompressed files and double-click the following file:
   - Linux UNIX `patch_installerGUI-`*`platform_number_of_bits`*`.sh`
   - Windows `patch_installerGUI-windows-x86_`*`number_of_bits`*`.bat`

   A splash screen opens. Click **OK**.
2. A Welcome panel opens. Click **Next**.
3. Provide the Tivoli Integrated Portal administrator ID and password, and click **Next**.
4. Click **Install** to apply the patches.
5. When the update completes, click **Done** to exit the wizard.

Results

You have updated Tivoli Integrated Portal, and WebSphere Application Server.

What to do next

To find out whether the interim fixes are installed, check the output from the following command:

- Linux UNIX *WAS_HOME*`/bin/versionInfo.sh -maintenancePackages`
- Windows *WAS_HOME*`\bin\versionInfo.bat -maintenancePackages`

Updating Tivoli Integrated Portal and WebSphere Application Server interactively in console mode using Patch Installer

Use the provided Patch Installer to interactively update the WebSphere Application Server in the console mode.

Before you begin

Copy the compressed Patch Installer from one of the DVDs or from Passport Advantage to a temporary directory on the computer where the administration server is installed, and uncompress the file.

Windows To successfully uncompress the file, use an archive manager other than the one built into Windows.

Procedure

1. Open the operating system command-line interface.
2. Enter the interactive mode of installation by running the following command:

- Linux UNIX `patch_installer-`*`platform`*`.sh -patchHome `*`location_of_patch_files`*
- Windows `patch_installer-`*`platform`*`.bat -patchHome `*`location_of_patch_files`*

-patchHome
Is the location of the patch files

3. Provide the values prompted on the console:

TIP_HOME
The location of Tivoli Integrated Portal 2.2.0.0 instance to be updated

Examples:

- UNIX Linux `TIP_HOME=/opt/IBM/TIP` - **embedded** WebSphere Application Server
- UNIX Linux `TIP_HOME=/opt/IBM/WebSphere/AppServer` - **base** WebSphere Application Server
- Windows `TIP_HOME=C:\\Program Files\\IBM\\TIP` - **embedded** WebSphere Application Server
- Windows `TIP_HOME=C:\\Program Files\\IBM\\WebSphere\\AppServer` - **base** WebSphere Application Server

TIP_ADMIN_NAME
The name of the Tivoli Integrated Portal administration user

TIP_ADMIN_PASSWORD
The password for the Tivoli Integrated Portal administration user

UPDI_HOME
The location of the WebSphere Update Installer instance that will be used to update the WebSphere Application Server on which the administration server is installed.

Tip: You can leave this parameter empty, because Patch Installer automatically chooses the most appropriate Update Installer instance on the computer. Provide the path to the chosen instance of Update Installer only if you want to override this default setting.

EXCLUDE_PACK_LIST
The fix or list of fixes that you want to exclude from the update process.

Tip:
- Leave this parameter empty if you want to apply all the fixes.
- If you want to exclude more than one fix, separate the fix names with a semicolon.

Results

You updated the server successfully.

What to do next

To find out whether the interim fixes are installed, check the output from the following command:

- Linux UNIX *WAS_HOME*/bin/versionInfo.sh -maintenancePackages
- Windows *WAS_HOME*\bin\versionInfo.bat -maintenancePackages

Updating Tivoli Integrated Portal and WebSphere Application Server in silent mode using Patch Installer

Use the provided Patch Installer to silently update Tivoli Integrated Portal, and WebSphere Application Server with important fix packs and interim fixes.

Before you begin

Copy the compressed Patch Installer from one of the DVDs or from Passport Advantage to a temporary directory on the computer where the administration server is installed, and uncompress the file.

Windows To successfully uncompress the file, use an archive manager other than the one built into Windows.

Procedure

1. Open the operating system command-line interface.
2. Generate a sample response file that will be used during the update:

- Linux UNIX patch_installer*platform*.sh -patchHome *location_of_patch_files* -genResponse *path_to_response_file*
- Windows patch_installer*platform*.bat -patchHome *location_of_patch_files* -genResponse *path_to_response_file*

where

-patchHome
Provide the full path to Patch Installer directory. This parameter is mandatory for every execution.

-genResponse *path_to_response_file*
Generate sample installation response file and exit. This response file must be edited before using.

3. Edit the generated response file specifying the following parameters:

TIP_HOME
The location of Tivoli Integrated Portal 2.2.0.0 instance to be updated

Examples:

embedded WebSphere Application Server	UNIX Linux `TIP_HOME=/opt/IBM/TIP` Windows `TIP_HOME=C:\\Program Files\\IBM\\TIP`
base WebSphere Application Server	UNIX Linux `TIP_HOME=/opt/IBM/WebSphere/AppServer` Windows `TIP_HOME=C:\\Program Files\\IBM\\WebSphere\\AppServer`

TIP_ADMIN_NAME
The name of the Tivoli Integrated Portal administration user

TIP_ADMIN_PASSWORD
The password for the Tivoli Integrated Portal administration user

UPDI_HOME
The location of the WebSphere Update Installer instance that will be used to update the WebSphere Application Server on which the administration server is installed.

Tip: You can leave this parameter empty, because Patch Installer automatically chooses the most appropriate Update Installer instance on the computer. Provide the path to the chosen instance of Update Installer only if you want to override this default setting.

EXCLUDE_PACK_LIST
The fix or list of fixes that you want to exclude from the update process.

Tip:
- Leave this parameter empty if you want to apply all the fixes.
- If you want to exclude more than one fix, separate the fix names with a semicolon.

4. Update the administration server by entering the following command:

- Linux UNIX `patchtool.sh -patchHome` *location_of_patch_files* `-response` *path_to_response_file* `-silent`
- Windows `patchtool.bat -patchHome` *location_of_patch_files* `-response` *path_to_response_file* `-silent`

You might also want to specify additional parameters:

-response
Read parameters from a particular installation response file. If you do not provide **response** and **genResponse** options, you will enter console interactive mode of the installation.

-silent Enforce the unattended mode of installation.

-log *path_to_log_file*
Provide the name of the file, including the full path to it if you want to redefine the default log name and its path.

-locale *language*
Enforce the use of a particular language. If the chosen language is not supported, "en_US" will be used.

-version
Prints version of the Patch Tool and quits

-help, -info, -?
Display this help and exit.

Results

You have updated the server successfully.

What to do next

To find out whether the interim fixes are installed, check the output from the following command:

- Linux UNIX *WAS_HOME*`/bin/versionInfo.sh -maintenancePackages`
- Windows *WAS_HOME*`\bin\versionInfo.bat -maintenancePackages`

Applying important updates manually

Install Tivoli Integrated Portal fix pack 2.2.0.3 and important WebSphere Application Server interim fixes manually.

Installing Tivoli Integrated Portal fix pack 2.2.0.3:

Tivoli Integrated Portal 2.2.0.3 fix pack can only be installed in silent mode, using a response file, at the command line. The silent installation uses a response file that is included with your fix pack media that you can edit as needed.

About this task

Important: This fix pack is installed in a Tivoli Integrated Portal Version 2.2 environment only.

Additionally, the following requirements and restrictions must be considered when you install this fix pack:

- If you installed the administration server on base WebSphere Application Server (Version 7.0), you must install fix pack 19 on the application server. WebSphere Application Server hardware and software requirements apply. For more information about hardware and software requirements, see: Hardware and software requirements.
- Ensure that you have installed the IBM version of Java Runtime Environment (JRE) 1.6.0 and that there at least 500 MB of disk space available in the temp directory for the installation process. You can also use the Java Runtime Environment installed with License Metric Tool.
- Before you install the fix pack, you must stop any Tivoli Integrated Portal-related Java processes that are running on your system.
  - UNIX Linux Use the `ps` command to view details of the Java processes that are running.
  - Windows Use a services utility to view the paths associated with each Java process.

The fix pack silent installation proceeds automatically, using the settings as they are specified in a response file (for example, `sample_response.txt`). Before you run the installation, edit this file to specify the choices and values to be used by the fix pack silent installer.

Procedure

1. Open your response file in a text editor and review the configuration settings. Edit as needed, then save and close the file.
2. At the command line, change to directory that contains your response file.
3. Enter the following at the command line:
   - UNIX Linux `./install.sh -i silent -f path_to_response_file`
   - Windows `install.bat -i silent -f path_to_response_file`

   Note: For systems running Microsoft Windows Vista or Microsoft Windows Server 2008, you must run `install.bat` as an administrator, that is, right click the command file (or a shortcut to it) and select **Run as administrator** before you run the installation command.

What to do next

After the installation, the Tivoli Integrated Portal administrator and any registered users can log in to the Tivoli Integrated Portal by entering the URL in a browser, for example, if you installed using default port numbers, you would access the console using the following web address: `http://localhost:16310/ibm/console`

The passwords entered in the response file can be seen by anyone who reads the file. When you are done using this file, delete it or move it to a secure place to keep passwords secure.

Silent mode response file parameters for fix pack 2.2.0.3:

The passwords entered in the response file can be seen by anyone who reads the file. When you are done using this file, delete it or move it to a secure place to keep passwords secure.

The following parameters are required for all installations of IBM License Metric Tool, regardless of whether you are installing the server, the database or both.

Table 31. Response file parameters for Tivoli Integrated Portal fix pack 2.2.0.3

Parameter	Parameter key name	Default
	Description	
The use of the silent installation method	**INSTALLER_UI**	SILENT
	This parameter indicates that Tivoli Integrated Portal is to be installed in silent mode and it should not be altered.	
The location of the existing Tivoli Integrated Portal 2.2.0.0 instance	**IAGLOBAL_TIP_HOME**	tip_home_dir
	• If the existing Tivoli Integrated Portal 2.2.0.0 instance is not associated with a WebSphere Application Server base installation, specify the location of the existing Tivoli Integrated Portal 2.2.0.0 instance. The default directory provided is: – UNIX Linux `/opt/IBM/tivoli/tipv2` – Windows `C:\\IBM\\tivoli\\tipv2` The \ backslash is seen as an escape character. Use \\ 2 backslashes when defining the path. • If the existing Tivoli Integrated Portal instance is associated with a WebSphere Application Server base installation, you must specify the location of the WebSphere Application Server base installation. For example: – UNIX Linux `/opt/IBM/WebSphere/AppServer` – Windows `C:\\IBM\\WebSphere\\AppServer`. The \ backslash is seen as an escape character. Use \\ 2 backslashes when defining the path.	
WebSphere Application Server user ID	**IAGLOBAL_WASUserID**	tip_admin_ID
	This parameter is for defining the administrator ID for the application server profile. The **tipadmin** user ID is provided by default, which you can change to another name.	
WebSphere Application Server user password	**IAGLOBAL_WASPassword**	password
	The password entered here will be required when you log in to the portal. **Note:** The password parameter must not be left blank, or start with a hyphen (-).	
Home directory for WebSphere Application Server Update Installer	**IAGLOBAL_UPDI_HOME**	UPDI_home_dir
	Important: This setting is for advanced users and typically no path needs to be specified.	

Table 31. Response file parameters for Tivoli Integrated Portal fix pack 2.2.0.3 (continued)

Parameter	Parameter key name	Default
	Description	
Operating system prerequisite checking	**IAGLOBAL_enableOSPrereqChecking**	false
	Important: This setting is for advanced users and typically you can accept the default setting (false). This parameter, when set to true enables operating system prerequisite checking, and allows the installation to continue and log warnings even if prerequisite checking fails.	
Installation components	**IAGLOBAL_COI_SELECTED_LOGICAL_COMPONENTS**	Common,TIPFinal
	This parameter indicates which components are to be installed. You must at least include the default values (Common,TIPFinal). Ensure that the additional components are available to the installer at cdimage/COI/PackageSteps. For example, to install the BIRTExtension component enter a value of Common,TIPFinal,BIRTExtension.	
The locale of the resource bundle	**IAGLOBAL_LOCALE**	en
	This parameter indicates the locale of the resource bundle for the installation.	

Manually applying interim fixes for WebSphere Application Server:

Use Update Installer to install the important interim fixes manually, and not by means of the Patch Installer.

Before you begin

Download and install Update Installer. It is available on the following website: IBM support. If you have an earlier version of Update Installer on your computer, you must uninstall it before installing this one.

Prepare the interim fix files: copy the Patch Tool zip file to a temporary directory, for example to *patchtool_install_dir*/maintenance/, from the product DVD or download from Passport Advantage, and uncompress it.

Table 32. Required interim fixes

Update	WebSphere Application Server	File name
Global Security Toolkit interim fix	embedded	7.0.0.0-WS-WASJavaSDK-*platform*-IFPM47413.pak
	base	7.0.0.0-WS-WASJavaSDK-*platform*-IFPM45367.pak
WebSphere Application Server interim fix for error 500	embedded	7.0.0.17-WS-WASEmbeded-IFPM34374.pak

The files are in the updates directory on the product DVD.

About this task

Perform the following steps to install the required interim fixes.

Procedure

1. Stop WebSphere Application Server.
2. Change to the temporary directory where you store the updates.
3. Run Update installer.
4. On the **Welcome panel**, read what products are supported and click **Next**.

5. Specify the path to the WebSphere installation directory, for example:
   - UNIX Linux `/opt/IBM/WebSphere/AppServer`
   - Windows `C:\Program Files\IBM\WebSphere\AppServer`
6. Select **Install maintenance package**, and click **Next**.
7. Enter the name of the temporary directory where you had placed the updates.
8. On the **Available Maintenance Package to install** page, select the appropriate files and click **Next**.
9. On the new panel click **Install**.
10. On the last page, click **Finish**. The packages are installed.
11. Start WebSphere Application Server.

Installing License Metric Tool 7.5 fix pack 1

Perform the following steps to install License Metric Tool 7.5 fix pack 1. Agents must be upgraded to the latest version after License Metric Tool 7.5 fix pack 1 is installed.

Before you begin

- A previous version of License Metric Tool 7.5 must be installed before you install License Metric Tool 7.5 fix pack 1.
- If you have interim fix 1 (IF0001) or interim fix 2 (IF0002) installed, you must install interim fix 3 (IF0003) before you install fix pack 1.

Step 1: Installing Tivoli Integrated Portal fix pack 2.2.0.7

Tivoli Integrated Portal 2.2.0.7 fix pack can only be installed in silent mode, using a response file, at the command line. The silent installation uses a response file that is included with your fix pack media that you can edit as needed.

About this task

Important: This fix pack is installed in a Tivoli Integrated Portal Version 2.2 environment only.

The fix pack silent installation proceeds automatically, using the settings as they are specified in a response file (for example, `sample_response.txt`). Before you run the installation, edit this file to specify the choices and values to be used by the fix pack silent installer. To find out solutions to some common problems that might occur during the installation, see the troubleshooting of Tivoli Integrated Portal fix pack 2.2.0.7 installation.

Procedure

1. Download the **FITSuit** tool version 3 or newer for Tivoli Integrated Portal fix pack 2.2.0.7 from the fix central for Tivoli Integrated Portal FP7. The same package is used for all operating systems:
   - `2.2.0-TIV-TIP-FITSuit-FP0007v3`
2. Extract the contents of the compressed file into a temporary directory.

   Tip:

   Windows When you copy and paste the contents of the compressed file or use the embedded Windows archiver to uncompress the file, the file might be incorrectly extracted. To ensure that the contents of the file is properly extracted, right-click on the compressed file and click **Extract All**.

Windows To avoid problems caused by long path names, extract the file to the main directory `C:\`.

3. Copy the `fit` directory that contains the extracted files to the `etc` directory that is in the Tivoli Integrated Portal profile, for example:

   Windows `C:\Program Files\IBM\TIP\profiles\TIPProfile\etc\fit`

   Linux `C:/opt/IBM/TIP/profiles/TIPProfile/etc/fit`

4. Download Tivoli Integrated Portal fix pack 2.2.0.7 from the fix central for Tivoli Integrated Portal FP7. Choose the package that matches your operating system:

   - AIX `2.2.0-TIV-TIP-AIXPPC64-FP0007`
   - HP-UX `2.2.0-TIV-TIP-HPUX64-FP0007`
   - Linux `2.2.0-TIV-TIP-Linux32-FP0007`
   - Linux `2.2.0-TIV-TIP-Linux64-FP0007`
   - Linux `2.2.0-TIV-TIP-LinuxPPC64-FP0007`
   - Linux `2.2.0-TIV-TIP-zLinux64-FP0007`
   - Solaris `2.2.0-TIV-TIP-SolarisSparc64-FP0007`
   - Windows `2.2.0-TIV-TIP-Windows32-FP0007`
   - Windows `2.2.0-TIV-TIP-Windows64-FP0007`

5. Extract the contents of the compressed file into a temporary directory.
6. Open the `sample_response.txt` file in a text editor and review the configuration settings. Uncomment the necessary lines and provide the following Tivoli Integrated Portal parameters:
   - Administrator user name and password
   - Home directory

   For example:

   - Windows

     `IAGLOBAL_TIP_HOME=C:\\Program Files\\IBM\\TIP9` (embedded WebSphere Application Server)

     `IAGLOBAL_TIP_HOME=C:\\Program Files\\IBM\\WebSphere\\AppServer` (base WebSphere Application Server)

     `IAGLOBAL_WASUserID=tipadmin`

     `IAGLOBAL_WASPassword=tippass`

   - Linux

     `IAGLOBAL_TIP_HOME=C:opt/IBM/TIP9` (embedded WebSphere Application Server)

     `IAGLOBAL_TIP_HOME=C:opt/IBM/WebSphere/AppServer` (base WebSphere Application Server)

     `IAGLOBAL_WASUserID=tipadmin`

     `IAGLOBAL_WASPassword=tippass`

   Restriction:

   - The password should not be empty or have a dash (-) as the first character.
   - Windows You must use an uppercase letter to denote a disk drive; otherwise the installation fails.

- Windows You must enter the Tivoli Integrated Portal directory in the same case that you used during the installation of the GA version of the application.

7. At the command line, change to the directory that contains your response file.
8. Enter the following at the command line:
   - UNIX Linux `./install.sh -i silent -f path_to_response_file`
   - Windows `install.bat -i silent -f path_to_response_file`

   Note:

   For systems running Microsoft Windows Vista or Microsoft Windows Server 2008, you must run `install.bat` as an administrator. Right click the command file (or a shortcut to it) and select **Run as administrator** before you run the installation command.

   For non-English installations:

   - UNIX Linux English is required as the system locale in the console where the fix pack installation is run.
   - Windows English is required as the system locale and as the default input language. Change language settings with Region and Language options in the Windows Control Panel.

Step 2: Updating WebSphere Application Server with important interim fixes

After installing Tivoli Integrated Portal fix pack 2.2.0.7, you must update WebSphere Application Server with critical security interim fixes.

Before you begin

- Verify the version of WebSphere Application Server using the **versionInfo** command.
- Download and install Update Installer. It is available on the following website: IBM support. If you have an earlier version of Update Installer on your computer, you must uninstall it before installing this one.
- Download one of the following packages from the fix central website:

• `7.5.0-TIV-ILMT-TAD4D-Embeded-WAS-IFixes.zip` • `7.5.0-TIV-ILMT-TAD4D-Embeded-WAS-IFixes.tar.gz`	embedded WebSphere Application Server
• `7.5.0-TIV-ILMT-TAD4D-WAS-IFixes.zip` • `7.5.0-TIV-ILMT-TAD4D-WAS-IFixes.tar.gz`	base WebSphere Application Server

Procedure

1. Copy the downloaded WebSphere Application Server interim fix files to the maintenance directory on the computer where the administration server is installed, for example:
   - Windows `C:\Program Files\IBM\TIP\WebSphereUpdateInstallerV7\maintenance`
   - Linux `/opt/IBM/TIP/WebSphereUpdateInstallerv7/maintenance`
2. Stop the IBM License Metric Tool server.
3. Start the Update Installer application.

4. On the **Welcome panel**, read what products are supported and click **Next**.
5. Specify the path to the WebSphere installation directory, for example:
   For the Base WebSphere Application Server
   - UNIX Linux `/opt/IBM/WebSphere/AppServer`
   - Windows `C:\Program Files\IBM\WebSphere\AppServer`

   For the Embedded WebSphere Application Server
   - UNIX Linux `/opt/IBM/TIP`
   - Windows `C:\Program Files\IBM\TIP`
6. Select **Install maintenance package**.
7. Enter the name of the directory where you copied the interim fix files.
8. On the **Available Maintenance Package to install** page, select the three updates and click **Next**.
9. Click **Install**.
10. On the last page, click **Finish**. The packages are installed.
11. Start the IBM License Metric Tool server.

What to do next

To find out whether the interim fixes are installed, check the output from:

- Linux UNIX *WAS_HOME*`/bin/versionInfo.sh -maintenancePackages`
- Windows *WAS_HOME*`\bin\versionInfo.bat -maintenancePackages`

Example:

```
/opt/IBM/WebSphere/AppServer/bin/versionInfo.sh -maintenancePackages
```

Step 3: Installing DB2 fix packs

Before you install License Metric Tool fix pack 1, you must install the required fix pack of DB2.

About this task

You must install the following fix packs, depending on the version of DB2 that you are using:

- If you are using DB2 Enterprise Server Edition server version 9.7, install fix pack 6 or higher.
- If you are using DB2 Enterprise Server Edition server version 9.5, install fix pack 10 or higher.
- If you are using DB2 Enterprise Server Edition server version 9.1, install fix pack 12 or higher.

The following procedure is a sample guideline that concerns the installation of the fix pack for DB2 version 9.7. It might not exactly fit the needs of patching your DB2 implementation. The procedure of installing DB2 fix packs is provided in the Information Centers for the particular versions of DB2. To install the fix packs, use the official DB2 documentation that is available under the following links:

- DB2 version 9.7 Information Center
- DB2 version 9.5 Information Center
- DB2 version 9.1 Information Center

Procedure

1. To install the DB2 fix pack on Linux or UNIX:
   a. Log in to the computer as root.
   b. Ensure that you meet all software, hardware, and operating system prerequisites.
   c. Download the universal fix pack that is suitable for your operating system.
   d. Extract the fix pack file.
   e. Stop the database.
   f. Install the fix pack.
   g. Perform the required post-installation tasks.
2. To install the DB2 fix pack on Windows:
   a. Log in to the computer as Administrator.
   b. Ensure that you meet all software, hardware, and operating system prerequisites.
   c. Download the universal fix pack that is suitable for your operating system.
   d. Extract the fix pack file.
   e. Stop the database.
   f. Install the fix pack by using a default method for a single database product. If you are not using a single database product, choose an installation method that better meets your requirements.
   g. Perform the required post-installation tasks.

Step 4: Installing License Metric Tool 7.5 fix pack 1

Install License Metric Tool 7.5 fix pack 1 to be able to use the service providers functionality, and resource value unit (RVU) licensing.

Before you begin

- You must have the following operating system privileges:
  - UNIX Linux `root`
  - Windows `Administrator`.
- On Windows 2008 server, run the installer by using the menu entry **Run as Administrator**.
- On UNIX and Linux server computers, there must be graphical interface available, and the X server must be properly configured (the *DISPLAY* variable must be set properly).

About this task

This task can be performed interactively or silently.

Interactively installing fix pack 1:
Procedure

1. Download fix pack 1 for License Metric Tool from the fix central website.
2. Place all the downloaded installation images in a single directory on the computer on which you are running the installer. For example:
   - Linux UNIX
     `/install_images`
   - Windows
     `C:\install_images`

Restriction: The path to the directory in which you place the installation images cannot contain the following characters: (space) ( )

3. In the directory where you extracted the installation files, run **launchpad.exe** (Windows) or **launchpad.sh** (other platforms). The Welcome page opens.

   Important: The Croatian language version is not supported by the launchpad, and the English version is displayed. After the installation, Croatian language version of the user interface is available.
4. In the left navigation bar, click **Install or upgrade to IBM License Metric Tool 7.5 fix pack 1**.
5. Click **Launch the server installation wizard**. A splash screen opens.

   Tip: You can also open the installation file:

   - UNIX Linux `ILMT-server-7.5.0.10-`*`your_platform`*`.sh` or
   - Windows `ILMT-server-7.5.0.10-`*`your_platform`*`.bat`

   in the *`extracted_installation_files`*`\server`. You do not need the web browser for this method.
6. The welcome screen opens. Click **Next**.
7. Provide the login and password for the Tivoli Integrated Portal administrator and click **Next**. A checklist pane with the results of DB2 validation opens. Click **Next**.

   Important: This panel is displayed only when you are migrating both the server and the database. It is not displayed if you are migrating only the database.
8. Provide the password for the `tlmsrv` user. After you click **Next**, the password is validated for correctness. Additionally, the installation wizard searches for the existing server database in the selected DB2 instance and verifies whether it can be used. Click **Next**.
9. On the installation summary page, check the information that is provided and confirm that you have enough space to complete the fix pack installation. Click **Install** to install the fix pack. After the initial deployment of files, the panel with configuration steps appears, listing all configuration steps and indicating their completion as the configuration proceeds.
10. When the configuration ends, click **Done** to exit the wizard.
11. Log in to License Metric Tool and import the latest version of the software catalog. If you have the latest version already imported, you must import it again to allow License Metric Tool for uploading data for RVU calculation.

What to do next

After the installation, the Tivoli Integrated Portal administrator and any registered users can log on to the Tivoli Integrated Portal by entering the URL in a browser. For example, if you installed Tivoli Integrated Portal using default port numbers, you would access the console by the following web address: `http://localhost:16310/ibm/console`

The password that was entered in the response file can be seen by anyone who reads the file. When you are done with using this file, delete it or move it to a secure place to keep passwords secure.

Agents must be upgraded to the latest version.

Installing the fix pack silently:
Procedure

1. Edit the response file in a text editor providing the following parameters:
   - `RSP_TLM_TLMSRV_PASSWD=`*`password`*
   - `RSP_TIP_ADMIN_NAME=`*`administrator_name`* (Optional - default value will be used if the line is empty or commented.)
   - `RSP_TIP_ADMIN_PASSWD=`*`password`* (mandatory)
   - `RSP_DISABLE_DB_CONNECTION_TEST` (mandatory)
2. To start the installation, on the command line, run the following command:
   - Linux UNIX `ILMT-server-7.5.0.10-`*`your_platform`*`.sh –f` *`response_file_path`* `–i silent`

     Where *response_file_path* is the absolute path to the response file you are using.

     Example:

     ```
     ILMT-server-7.5.0.10-linux-ppc64.sh -f /install_images/server/
     installResponseProduction.txt -i silent
     ```
   - Windows `ILMT-server-7.5.0.10-`*`your_platform`*`.bat –f` *`response_file_path`* `–i silent`

     Where *response_file_path* is the absolute path to the response file you are using.

     Example:

     ```
     ILMT-server-7.5.0.10-windows-x86_64.bat -f c:\image\server\
     installResponseProduction.txt -i silent
     ```
3. Log in to License Metric Tool and import the latest version of the software catalog. If you have the latest version already imported, you must import it again to allow License Metric Tool for uploading data for RVU calculation.

What to do next

After the installation, the Tivoli Integrated Portal administrator and any registered users can log on to the Tivoli Integrated Portal by entering the URL in a browser. For example, if you installed Tivoli Integrated Portal using default port numbers, you would access the console by the following web address: `http://localhost:16310/ibm/console`

The password that was entered in the response file can be seen by anyone who reads the file. When you are done with using this file, delete it or move it to a secure place to keep passwords secure.

Agents must be upgraded to the latest version.

Verifying the server installation

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

About this task

The log files together with the web UI based on Tivoli Integrated Portal contain information that helps you check if the application server has been successfully installed. You can access the web UI using Mozilla Firefox or Internet Explorer web browser.

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

All installation logs are compressed and stored in the application directory. If the file has not been created there, it can be found in the temporary directory:

- UNIX Linux `/tmp`
- Windows `%temp%`

The compressed file is created only if you run the installation from the launchpad interface or run the installer file:

- UNIX Linux `ILMT-server-7.5-`*`platform`*`.sh`
- Windows `ILMT-server-7.5-`*`platform`*`.bat`

You can send this log to IBM support in case of complicated installation problems. Example file name: `LMT_7.5_20110607-113235_19446_logs.tar.gz`.

Procedure

1. Open the `msg_servers.log` file and check if it contains the 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: `https://`*`adm_server_IP_addr`*`:16311/ibm/console/logon.jsp` and check the Tivoli Integrated Portal 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 You can also open the login page from the system **Start** menu.

Setting memory for Java client processes

The default settings for the Java heap size might not be sufficient for large environments. You can increase the memory available to Java client processes by increasing the Java heap size. By default, the maximum heap size is 1024 MB.

If a Java client process requires an extensive use of memory and the default Java heap size is insufficient, then the process can fail with an `OutOfMemoryError` Java exception.

This error can occur when:

- Data is being aggregated
- The catalog is being imported
- Aggregated data is recalculated

For more information see the topic Tuning the IBM virtual machine for Java in the WebSphere Application Server V7.0 information center.

Perform the following steps to increase the Java heap size:

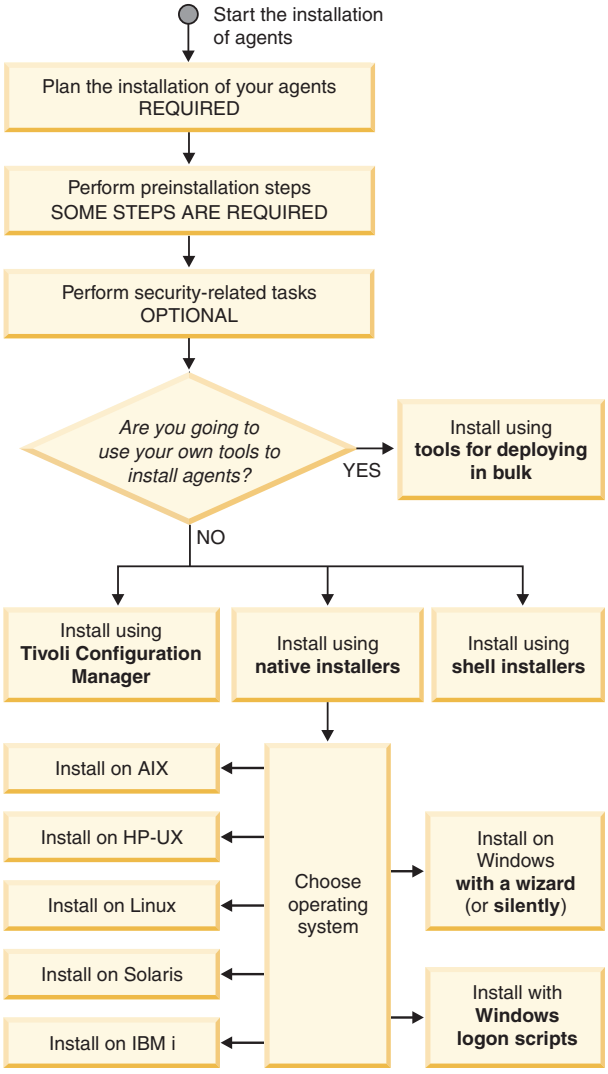
1. From the Tivoli Integrated Portal, select **Settings** > **WebSphere Administrative Console**.
2. Click **Launch WebSphere Administrative Console**.
3. Select **Servers** > **Server Types** > **WebSphere application servers**.

4. In the Server Infrastructure section, select **Java and process management** > **Process definition**.
5. In the Additional Properties section, select **Java Virtual Machine**.
6. Specify new values for the **Initial heap size** and the **Maximum heap size** fields.

Chapter 3. Installing agents

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

About this task



1. Plan the installation of your agents. Most importantly, check the agents hardware and software prerequisites, virtualization considerations, and other software requirements for the agents (**required**)
2. Perform agent preinstallation tasks (**optional**)

   Depending on your software and the security level you selected, there are several tasks you must perform before you install the agents. For example, if you are going to use secure communications, you must enable a valid certificate for the server and agents.
3. Performing agent security-related tasks. (**optional**)

   Depending on your software and the security level you selected while installing the administration server, there are several tasks you need to perform before you install the agents.
4. Install agents on computers that you want to monitor (**required**) IBM License Metric Tool provides several methods for installing the agents on the computers that you want to monitor.

   Agent installation methods:

   - You might want to use your own tools to install agents in bulk. This method is intended for advanced administrators who want to write their own scripts or use existing commercial tools for installing a lot of agents. It uses native installers.
   - Install with Tivoli Configuration Manager. This method is available on all supported platforms and is suitable for environments where Configuration Manager is installed.
   - Install with native installers. You can also install agents silently.

     Supported platforms: AIX, HP-UX, IBM i, Linux, Linux on System z, Solaris, and Windows.

     You might also want to install agents with Windows Logon Scripts. This method is suitable for topologies where Windows agents are to be installed.
   - Install with shell installers (UNIX platforms only). It is not necessary to edit and copy the response file to the target directory. All the parameters that you supply are validated on the run.

   If any problems have occurred, start troubleshooting the agent installations.

Planning the installation of agents

The topics in this section contain information about hardware and software prerequisites that need to be fulfilled when installing License Metric Tool agents. The requirements were determined in previous releases of License Metric Tool.

About this task

1. "Supported operating systems for agents"

   Ensure that the computer where you are installing the agent runs on one of the supported operating systems.
2. "Other software requirements for the agents" on page 90

   Ensure that the corequisite software is installed on the computer where you are installing the agent.
3. "VMware and Microsoft virtualization considerations" on page 92

   Both the server and agents can be installed on 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.
4. "Disk space requirements" on page 93

   Before deploying the IBM License Metric Tool agents, and the WebSphere agent, ensure that your machine has the required amount of disk space.
5. "Support for high availability environments" on page 97

   This topic provides information about the conditions in which monitoring of high availability environments, managed by IBM High Availability Cluster Multiprocessing, has been validated.
6. "Supported national languages for IBM i agents" on page 99

   You must install one of the supported languages as your primary or secondary language on the IBM i node.

Supported operating systems for agents

Ensure that the computer where you are installing the agent runs on one of the supported operating systems.

To check whether your agent operating system is supported, click:

"AIX" on page 81 | "HP-UX" on page 82 | "IBM i" on page 82 | "Oracle Solaris" on page 82 | "Red Hat Enterprise Linux" on page 83 | "Red Hat Linux Desktop" on page 86 | "Novell Linux Desktop" on page 85 | "SUSE Linux Enterprise Server" on page 86 | "SUSE Linux Enterprise Desktop" on page 87 | "Windows" on page 88

AIX

Version	Required level, service packs, patches	Supported partitioning technologies
7.1		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) LPAR mobility (Live Partition Mobility) WPAR mobility (Live Application Mobility) IBM zEnterprise® BladeCenter® Extension (zBX) Processor Core Deconfiguration
6.1	APAR IZ49636 - this fix is required if you are installing the agent in a WPAR environment. If you are installing the agent in a WPAR environment and using WPAR or LPAR mobility or relocation, the AIX 6.1 instance needs to be upgraded to Technology Level 3 or later. 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) LPAR mobility (Live Partition Mobility) WPAR mobility (Live Application Mobility) IBM zEnterprise BladeCenter Extension (zBX) Processor Core Deconfiguration
5.3	xlC.aix50.rte.6.0.0.3 or later Maintenance Level 3 to support sub capacity pricing on Power® 5 **Note:** Maintenance Level 3 is a minimum requirement, but use Technology 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 (Live Partition Mobility) IBM zEnterprise BladeCenter Extension (zBX) Processor Core Deconfiguration
5.2	xlC.aix50.rte.6.0.0.3 or later APAR IY51805 procfiles	LPAR PowerVM - Single Shared Processor Pool

License Metric Tool agents can also be deployed on Virtual I/O Server (VIOS) version 2.2.1 and higher. The deployment procedure is the same as the standard one. For more information, see “Installing agents on AIX using native installers” on page 110.

HP-UX

Version	Required level, service packs, patches	Supported partitioning technologies
11i v3 on PA-RISC		nPAR vPAR (all except for version 6)
11i v2 on PA-RISC 64-bit (in 32-bit compatibility mode)	Quality Pack Depot for 11i v2, September 2006 • PHKL_35709 (s700_800 11.23 pthread_cond_timedwait, hires timers, callout) • PHCO_39699 (s700_800 11.23 pthread library cumulative patch)	
11i v3 on Itanium 2 Integrity Server		HP Integrity Virtual Machines 3.5 HP Integrity Virtual Machines 4.0 HP Integrity Virtual Machines 4.1 HP Integrity Virtual Machines 4.2 HP Integrity Virtual Machines 4.3 nPAR vPAR (all except for version 6) iCAPv9
11i v2 on Itanium 2 Integrity Server	Quality Pack Depot for 11i v2, September 2006 • PHKL_35709 (s700_800 11.23 pthread_cond_timedwait, hires timers, callout) • PHCO_39699 (s700_800 11.23 pthread library cumulative patch)	

IBM i

Version	Required level, service packs, patches	Supported partitioning technologies
V7R1	PTF SI39319 PTF SI38154 for 5770SS1 Options 13 and 30 of 5770SS1	LPAR PowerVM - DLPAR PowerVM - Single Shared Processor Pool PowerVM - Micro-Partitioning PowerVM - Multiple Shared Processor Pools PowerVM - Shared Dedicated Processor
V6R1	PTF SI39046 PTF SI38115 for 5761SS1 Options 13 and 30 of 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	PTF SI38116 for 5722SS1 Options 13 and 30 of 5722SS1 Crypto Access Provider 128-bit, PID: 5722AC3 (if secure communication is to be used)	

Oracle Solaris

Version	Required level, service packs, patches	Supported partitioning technologies
11 Operating System for x86 (64-bit)		Containers/Zones BIOS (SMBIOS 2.5 or higher) & Operating System boot core limit

Version	Required level, service packs, patches	Supported partitioning technologies
11 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. Dynamic Domains. Solaris in Dynamic 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 and Dynamic Domains Containers/Zones: node OS Logical Domains - LDOMs (Oracle VM Server for SPARC 2.0) Containers/Zones: inside Logical Domains
10 Operating System for x86 (64-bit)		Containers/Zones BIOS (SMBIOS 2.5 or higher) & Operating System boot core limit
10 Operating System for SPARC and UltraSPARC (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. Dynamic Domains. Solaris in Dynamic 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 and Dynamic Domains Containers/Zones: node OS Logical Domains - LDOMs (Oracle VM Server for SPARC 2.0) Containers/Zones: inside Logical Domains
9 Operating System for UltraSPARC (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. Dynamic Domains. Solaris in Dynamic 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.

Red Hat Enterprise Linux

Version	Required level, service packs, patches	Supported partitioning technologies
6 for Intel/AMD x86 (64-bit)	compat-libstdc++-33 (32 and 64-bit)	VMware ESX 4 - Single Server, Cluster, Mobility (VMware Vmotion) VMware ESXi 4 - Single Server, Cluster, Mobility (VMware Vmotion) VMware ESX 4.1 - Single Server, Cluster, Mobility (VMware Vmotion) VMware ESXi 4.1 - Single Server, Cluster, Mobility (VMware Vmotion) VMware vSphere 5 - Single Server, Cluster, Mobility (VMware Vmotion) VMware vSphere 5.1 - Single Server, Cluster, Mobility (VMware Vmotion) BIOS (SMBIOS 2.5 or higher) & Operating System boot core limit System scaling using Intel QuickPath Interconnect Fix Pack 1 Kernel-based Virtual Machine (KVM), on RHEV with RHEV-M (Red hat Linux Virtualization Manager) 3.0
6 for Intel/AMD x86 (32-bit)	compat-libstdc++-33 (32-bit)	VMware ESX 4 - Single Server, Cluster, Mobility (VMware Vmotion) VMware ESXi 4 - Single Server, Cluster, Mobility (VMware Vmotion) VMware ESX 4.1 - Single Server, Cluster, Mobility (VMware Vmotion) VMware ESXi 4.1 - Single Server, Cluster, Mobility (VMware Vmotion) VMware vSphere 5 - Single Server, Cluster, Mobility (VMware Vmotion) VMware vSphere 5.1 - Single Server, Cluster, Mobility (VMware Vmotion) BIOS (SMBIOS 2.5 or higher) & Operating System boot core limit System scaling using Intel QuickPath Interconnect Fix Pack 1 Kernel-based Virtual Machine (KVM), on RHEV with RHEV-M (Red hat Linux Virtualization Manager) 3.0

Version	Required level, service packs, patches	Supported partitioning technologies
6 for IBM Power Systems (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 (Live Partition Mobility) Processor Factory Deconfiguration
6 for IBM System z (64-bit) on 64-bit hardware	compat-libstdc++-33	LPAR z/VM®
5 for Intel/AMD x86 (64-bit)	compat-libstdc++-33 (32 and 64-bit)	VMware ESX 3.0 - Single Server, Cluster, Mobility (VMware Vmotion) VMware ESX 3.5 - Single Server, Cluster, Mobility (VMware Vmotion) VMware ESXi 3.5 - Single Server, Cluster, Mobility (VMware Vmotion) VMware ESX 4 - Single Server, Cluster, Mobility (VMware Vmotion) VMware ESXi 4 - Single Server, Cluster, Mobility (VMware Vmotion) VMware ESX 4.1 - Single Server, Cluster, Mobility (VMware Vmotion) VMware ESXi 4.1 - Single Server, Cluster, Mobility (VMware Vmotion) VMware vSphere 5 - Single Server, Cluster, Mobility (VMware Vmotion) VMware vSphere 5.1 - Single Server, Cluster, Mobility (VMware Vmotion) BIOS (SMBIOS 2.5 or higher) & Operating System boot core limit System scaling using Intel QuickPath Interconnect Microsoft Hyper-V R2 (can be stand alone or role) Fix Pack 1 Kernel-based Virtual Machine (KVM), on RHEV with RHEV-M (Red hat Linux Virtualization Manager) 3.0
5 for Intel/AMD x86 (32-bit)	compat-libstdc++-33 (32-bit)	VMware ESX 3.0 - Single Server, Cluster, Mobility (VMware Vmotion) VMware ESX 3.5 - Single Server, Cluster, Mobility (VMware Vmotion) VMware ESXi 3.5 - Single Server, Cluster, Mobility (VMware Vmotion) VMware ESX 4 - Single Server, Cluster, Mobility (VMware Vmotion) VMware ESXi 4 - Single Server, Cluster, Mobility (VMware Vmotion) VMware ESX 4.1 - Single Server, Cluster, Mobility (VMware Vmotion) VMware ESXi 4.1 - Single Server, Cluster, Mobility (VMware Vmotion) VMware vSphere 5 - Single Server, Cluster, Mobility (VMware Vmotion) VMware vSphere 5.1 - Single Server, Cluster, Mobility (VMware Vmotion) BIOS (SMBIOS 2.5 or higher) & Operating System boot core limit System scaling using Intel QuickPath Interconnect Microsoft Hyper-V R2 (can be stand alone or role) Fix Pack 1 Kernel-based Virtual Machine (KVM), on RHEV with RHEV-M (Red hat Linux Virtualization Manager) 3.0
5 for IBM Power Systems (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 (Live Partition Mobility) Processor Factory Deconfiguration
5 for IBM System z (64-bit) on 64-bit hardware	compat-libstdc++-33	LPAR z/VM

Version	Required level, service packs, patches	Supported partitioning technologies
ES/AS/WS 4 for Intel/AMD x86 (64-bit)	compat-libstdc++-33 (32 and 64-bit)	VMware ESX 3.0 - Single Server, Cluster, Mobility (VMware Vmotion) VMware ESX 3.5 - Single Server, Cluster, Mobility (VMware Vmotion) VMware ESXi 3.5 - Single Server, Cluster, Mobility (VMware Vmotion) VMware ESX 4 - Single Server, Cluster, Mobility (VMware Vmotion) VMware ESXi 4 - Single Server, Cluster, Mobility (VMware Vmotion) VMware ESX 4.1 - Single Server, Cluster, Mobility (VMware Vmotion) VMware ESXi 4.1 - Single Server, Cluster, Mobility (VMware Vmotion) VMware vSphere 5 - Single Server, Cluster, Mobility (VMware Vmotion) VMware vSphere 5.1 - Single Server, Cluster, Mobility (VMware Vmotion) BIOS (SMBIOS 2.5 or higher) & Operating System boot core limit System scaling using Intel QuickPath Interconnect Fix Pack 1 Kernel-based Virtual Machine (KVM), on RHEV with RHEV-M (Red hat Linux Virtualization Manager) 3.0
ES/AS/WS 4 for Intel/AMD x86 (32-bit)	Compatibility packs: 1. libgcc-3.4.3-9 (32-bit) 2. compat-libstdc++-33 (32-bit, must be installed in the specified order)	VMware ESX 3.0 - Single Server, Cluster, Mobility (VMware Vmotion) VMware ESX 3.5 - Single Server, Cluster, Mobility (VMware Vmotion) VMware ESXi 3.5 - Single Server, Cluster, Mobility (VMware Vmotion) VMware ESX 4 - Single Server, Cluster, Mobility (VMware Vmotion) VMware ESXi 4 - Single Server, Cluster, Mobility (VMware Vmotion) VMware ESX 4.1 - Single Server, Cluster, Mobility (VMware Vmotion) VMware ESXi 4.1 - Single Server, Cluster, Mobility (VMware Vmotion) VMware vSphere 5 - Single Server, Cluster, Mobility (VMware Vmotion) VMware vSphere 5.1 - Single Server, Cluster, Mobility (VMware Vmotion) BIOS (SMBIOS 2.5 or higher) & Operating System boot core limit System scaling using Intel QuickPath Interconnect Fix Pack 1 Kernel-based Virtual Machine (KVM), on RHEV with RHEV-M (Red hat Linux Virtualization Manager) 3.0
AS, version 4 for IBM Power Systems (64-bit)	Compatibility packs: 1. libgcc-3.4.3-9 (32-bit) 2. compat-libstdc++-33 (must be installed in the specified order)	LPAR PowerVM - DLPAR PowerVM - Single Shared Processor Pool PowerVM - Micro-Partitioning
AS, version 4 for IBM System z (64–bit)		LPAR z/VM
AS, version 4 for IBM System z (31-bit) on 64-bit hardware	compat-libstdc++-33 (32 and 64-bit)	LPAR z/VM

Novell Linux Desktop

Version	Required level, service packs, patches	Supported partitioning technologies
9 for Intel/AMD x86 (64-bit)	compat-libstdc++ (32 and 64-bit)	VMware ESX 3.0 - Single Server, Cluster, Mobility (VMware Vmotion) VMware ESX 3.5 - Single Server, Cluster, Mobility (VMware Vmotion) VMware ESXi 3.5 - Single Server, Cluster, Mobility (VMware Vmotion) VMware ESX 4 - Single Server, Cluster, Mobility (VMware Vmotion) VMware ESXi 4 - Single Server, Cluster, Mobility (VMware Vmotion) VMware ESX 4.1 - Single Server, Cluster, Mobility (VMware Vmotion) VMware ESXi 4.1 - Single Server, Cluster, Mobility (VMware Vmotion) VMware vSphere 5 - Single Server, Cluster, Mobility (VMware Vmotion) VMware vSphere 5.1 - Single Server, Cluster, Mobility (VMware Vmotion)

Version	Required level, service packs, patches	Supported partitioning technologies
9 for Intel/AMD x86 (32-bit)	compat-libstdc++ (32-bit)	VMware ESX 3.0 - Single Server, Cluster, Mobility (VMware Vmotion) VMware ESX 3.5 - Single Server, Cluster, Mobility (VMware Vmotion) VMware ESXi 3.5 - Single Server, Cluster, Mobility (VMware Vmotion) VMware ESX 4 - Single Server, Cluster, Mobility (VMware Vmotion) VMware ESXi 4 - Single Server, Cluster, Mobility (VMware Vmotion) VMware ESX 4.1 - Single Server, Cluster, Mobility (VMware Vmotion) VMware ESXi 4.1 - Single Server, Cluster, Mobility (VMware Vmotion) VMware vSphere 5 - Single Server, Cluster, Mobility (VMware Vmotion) VMware vSphere 5.1 - Single Server, Cluster, Mobility (VMware Vmotion)

Red Hat Linux Desktop

Version	Required level, service packs, patches	Supported partitioning technologies
version 6 for Intel/AMD x86 (64-bit)	compat-libstdc++-33 (32-bit)	VMware ESX 3.0 - Single Server, Cluster, Mobility (VMware Vmotion) VMware ESX 3.5 - Single Server, Cluster, Mobility (VMware Vmotion) VMware ESXi 3.5 - Single Server, Cluster, Mobility (VMware Vmotion)
version 6 for Intel/AMD x86 (32-bit)	compat-libstdc++-33 (32-bit)	VMware ESX 3.0 - Single Server, Cluster, Mobility (VMware Vmotion) VMware ESX 3.5 - Single Server, Cluster, Mobility (VMware Vmotion) VMware ESXi 3.5 - Single Server, Cluster, Mobility (VMware Vmotion)
version 5 for Intel/AMD x86 (32-bit)	compat-libstdc++-33 (32-bit)	VMware ESX 3.0 - Single Server, Cluster, Mobility (VMware Vmotion) VMware ESX 3.5 - Single Server, Cluster, Mobility (VMware Vmotion) VMware ESXi 3.5 - Single Server, Cluster, Mobility (VMware Vmotion)
version 4 for Intel/AMD x86 (32-bit)	compat-libstdc++-33 (32-bit)	VMware ESX 3.0 - Single Server, Cluster, Mobility (VMware Vmotion) VMware ESX 3.5 - Single Server, Cluster, Mobility (VMware Vmotion) VMware ESXi 3.5 - Single Server, Cluster, Mobility (VMware Vmotion)

SUSE Linux Enterprise Server

Version	Required level, service packs, patches	Supported partitioning technologies
11 for Intel/AMD x86 (64-bit)	libstdc++33-32bit-3.3.3-11.9.x86_64.rpm	VMware ESX 4 - Single Server, Cluster, Mobility (VMware Vmotion) VMware ESXi 4 - Single Server, Cluster, Mobility (VMware Vmotion) VMware ESX 4.1 - Single Server, Cluster, Mobility (VMware Vmotion) VMware ESXi 4.1 - Single Server, Cluster, Mobility (VMware Vmotion) VMware vSphere 5 - Single Server, Cluster, Mobility (VMware Vmotion) VMware vSphere 5.1 - Single Server, Cluster, Mobility (VMware Vmotion) BIOS (SMBIOS 2.5 or higher) & Operating System boot core limit System scaling using Intel QuickPath Interconnect Microsoft Hyper-V R2 (can be stand alone or role)
11 for Intel/AMD x86 (32-bit)		VMware ESX 4 - Single Server, Cluster, Mobility (VMware Vmotion) VMware ESXi 4 - Single Server, Cluster, Mobility (VMware Vmotion) VMware ESX 4.1 - Single Server, Cluster, Mobility (VMware Vmotion) VMware ESXi 4.1 - Single Server, Cluster, Mobility (VMware Vmotion) VMware vSphere 5 - Single Server, Cluster, Mobility (VMware Vmotion) VMware vSphere 5.1 - Single Server, Cluster, Mobility (VMware Vmotion) BIOS (SMBIOS 2.5 or higher) & Operating System boot core limit System scaling using Intel QuickPath Interconnect Microsoft Hyper-V R2 (can be stand alone or role)
11 for IBM Power Systems (64-bit)		LPAR PowerVM - DLPAR PowerVM - Single Shared Processor Pool PowerVM - Micro-Partitioning LPAR mobility (Live Partition Mobility) Processor Factory Deconfiguration

Version	Required level, service packs, patches	Supported partitioning technologies
11 for IBM System z (64-bit) on 64-bit hardware		LPAR z/VM
10 for Intel/AMD x86 (32-bit and 64-bit)	compat-libstdc++ (32 and 64-bit)	VMware ESX 3.0 - Single Server, Cluster, Mobility (VMware Vmotion) VMware ESX 3.5 - Single Server, Cluster, Mobility (VMware Vmotion) VMware ESXi 3.5 - Single Server, Cluster, Mobility (VMware Vmotion) VMware ESX 4 - Single Server, Cluster, Mobility (VMware Vmotion) VMware ESXi 4 - Single Server, Cluster, Mobility (VMware Vmotion) VMware ESX 4.1 - Single Server, Cluster, Mobility (VMware Vmotion) VMware ESXi 4.1 - Single Server, Cluster, Mobility (VMware Vmotion) VMware vSphere 5 - Single Server, Cluster, Mobility (VMware Vmotion) VMware vSphere 5.1 - Single Server, Cluster, Mobility (VMware Vmotion) Microsoft Hyper-V R1 (can be stand alone or role) Microsoft Hyper-V R2 (can be stand alone or role) BIOS (SMBIOS 2.5 or higher) & Operating System boot core limit System scaling using Intel QuickPath Interconnect
10 for IBM Power Systems (64-bit)	compat-libstdc++ Service Pack 1 for LPAR mobility	LPAR PowerVM - DLPAR PowerVM - Single Shared Processor Pool PowerVM - Micro-Partitioning LPAR mobility (Live Partition Mobility) Processor Factory Deconfiguration
10 for IBM System z (64-bit) on 64-bit hardware	compat-libstdc++	LPAR z/VM
9 for Intel/AMD x86 (64-bit)	Service pack 1 to support sub-capacity pricing on Power 5 compat-libstdc++ (32 and 64-bit)	VMware ESX 3.0 - Single Server, Cluster, Mobility (VMware Vmotion) VMware ESX 3.5 - Single Server, Cluster, Mobility (VMware Vmotion) VMware ESXi 3.5 - Single Server, Cluster, Mobility (VMware Vmotion) VMware ESX 4 - Single Server, Cluster, Mobility (VMware Vmotion) VMware ESXi 4 - Single Server, Cluster, Mobility (VMware Vmotion) VMware ESX 4.1 - Single Server, Cluster, Mobility (VMware Vmotion) VMware ESXi 4.1 - Single Server, Cluster, Mobility (VMware Vmotion) VMware vSphere 5 - Single Server, Cluster, Mobility (VMware Vmotion) VMware vSphere 5.1 - Single Server, Cluster, Mobility (VMware Vmotion) BIOS (SMBIOS 2.5 or higher) & Operating System boot core limit System scaling using Intel QuickPath Interconnect
9 for Intel/AMD x86 (32-bit)		VMware ESX 3.0 - Single Server, Cluster, Mobility (VMware Vmotion) VMware ESX 3.5 - Single Server, Cluster, Mobility (VMware Vmotion) VMware ESXi 3.5 - Single Server, Cluster, Mobility (VMware Vmotion) VMware ESX 4 - Single Server, Cluster, Mobility (VMware Vmotion) VMware ESXi 4 - Single Server, Cluster, Mobility (VMware Vmotion) VMware ESX 4.1 - Single Server, Cluster, Mobility (VMware Vmotion) VMware ESXi 4.1 - Single Server, Cluster, Mobility (VMware Vmotion) VMware vSphere 5 - Single Server, Cluster, Mobility (VMware Vmotion) VMware vSphere 5.1 - Single Server, Cluster, Mobility (VMware Vmotion) BIOS (SMBIOS 2.5 or higher) & Operating System boot core limit System scaling using Intel QuickPath Interconnect

SUSE Linux Enterprise Desktop

Version	Required level, service packs, patches	Supported partitioning technologies
11 for Intel/AMD x86 (32-bit)		BIOS (SMBIOS 2.5 or higher) & Operating System boot core limit
11 for Intel/AMD x86 (64-bit)		BIOS (SMBIOS 2.5 or higher) & Operating System boot core limit

Version	Required level, service packs, patches	Supported partitioning technologies
10 for Intel/AMD x86 (32-bit)		BIOS (SMBIOS 2.5 or higher) & Operating System boot core limit
10 for Intel/AMD x86 (64-bit)	compat-libstdc++ (32 and 64-bit)	BIOS (SMBIOS 2.5 or higher) & Operating System boot core limit

Windows

Version	Required level, service packs, patches	Supported partitioning technologies
8 Ultimate (32-bit and 64-bit) **8 Enterprise** (32-bit and 64-bit) **8 Professional** (32-bit and 64-bit)		VMware vSphere 5 - Single Server, Cluster, Mobility (VMware Vmotion) VMware vSphere 5.1 - Single Server, Cluster, Mobility (VMware Vmotion) Microsoft Hyper-V R2 (can be stand alone or role) BIOS (SMBIOS 2.5 or higher) & Operating System boot core limit
7 Ultimate (32-bit and 64-bit) **7 Enterprise** (32-bit and 64-bit) **7 Professional** (32-bit and 64-bit)		VMware ESX 4 - Single Server, Cluster, Mobility (VMware Vmotion) VMware ESXi 4 - Single Server, Cluster, Mobility (VMware Vmotion) VMware ESX 4.1 - Single Server, Cluster, Mobility (VMware Vmotion) VMware ESXi 4.1 - Single Server, Cluster, Mobility (VMware Vmotion) VMware vSphere 5 - Single Server, Cluster, Mobility (VMware Vmotion) VMware vSphere 5.1 - Single Server, Cluster, Mobility (VMware Vmotion) Microsoft Hyper-V R1 (can be stand alone or role) Microsoft Hyper-V R2 (can be stand alone or role) BIOS (SMBIOS 2.5 or higher) & Operating System boot core limit System scaling using Intel QuickPath Interconnect Fix Pack 1 Kernel-based Virtual Machine (KVM), on RHEV with RHEV-M (Red hat Linux Virtualization Manager) 3.0
Vista Ultimate (32-bit and 64-bit) **Vista Enterprise** (32-bit and 64-bit) **Vista Business** (32-bit and 64-bit)		VMware ESX 3.0 - Single Server, Cluster, Mobility (VMware Vmotion) VMware ESX 3.5 - Single Server, Cluster, Mobility (VMware Vmotion) VMware ESXi 3.5 - Single Server, Cluster, Mobility (VMware Vmotion) VMware ESX 4 - Single Server, Cluster, Mobility (VMware Vmotion) VMware ESXi 4 - Single Server, Cluster, Mobility (VMware Vmotion) VMware ESX 4.1 - Single Server, Cluster, Mobility (VMware Vmotion) VMware ESXi 4.1 - Single Server, Cluster, Mobility (VMware Vmotion) VMware vSphere 5 - Single Server, Cluster, Mobility (VMware Vmotion) VMware vSphere 5.1 - Single Server, Cluster, Mobility (VMware Vmotion) Microsoft Hyper-V R1 (can be stand alone or role) Microsoft Hyper-V R2 (can be stand alone or role) BIOS (SMBIOS 2.5 or higher) & Operating System boot core limit System scaling using Intel QuickPath Interconnect
Server 2012 Standard and Datacenter (64-bit)		VMware vSphere 5 - Single Server, Cluster, Mobility (VMware Vmotion) VMware vSphere 5.1 - Single Server, Cluster, Mobility (VMware Vmotion) Microsoft Hyper-V R2 (can be stand alone or role) BIOS (SMBIOS 2.5 or higher) & Operating System boot core limit

Version	Required level, service packs, patches	Supported partitioning technologies
Server 2008 R2 Standard, Enterprise, and Datacenter (64-bit) for Intel x86		VMware ESX 3.5 - Single Server, Cluster, Mobility (VMware Vmotion) VMware ESXi 3.5 - Single Server, Cluster, Mobility (VMware Vmotion) VMware ESX 4 - Single Server, Cluster, Mobility (VMware Vmotion) VMware ESXi 4 - Single Server, Cluster, Mobility (VMware Vmotion) VMware ESX 4.1 - Single Server, Cluster, Mobility (VMware Vmotion) VMware ESXi 4.1 - Single Server, Cluster, Mobility (VMware Vmotion) VMware vSphere 5 - Single Server, Cluster, Mobility (VMware Vmotion) VMware vSphere 5.1 - Single Server, Cluster, Mobility (VMware Vmotion) Microsoft Hyper-V R1 (can be stand alone or role) Microsoft Hyper-V R2 (can be stand alone or role) BIOS (SMBIOS 2.5 or higher) & Operating System boot core limit System scaling using Intel QuickPath Interconnect Fix Pack 1 Kernel-based Virtual Machine (KVM), on RHEV with RHEV-M (Red hat Linux Virtualization Manager) 3.0
Server 2008 Standard and Enterprise (32-bit and 64-bit) for Intel x86		VMware ESX 3.5 - Single Server, Cluster, Mobility (VMware Vmotion) VMware ESXi 3.5 - Single Server, Cluster, Mobility (VMware Vmotion) VMware ESX 4 - Single Server, Cluster, Mobility (VMware Vmotion) VMware ESXi 4 - Single Server, Cluster, Mobility (VMware Vmotion) VMware ESX 4.1 - Single Server, Cluster, Mobility (VMware Vmotion) VMware ESXi 4.1 - Single Server, Cluster, Mobility (VMware Vmotion) VMware vSphere 5 - Single Server, Cluster, Mobility (VMware Vmotion) VMware vSphere 5.1 - Single Server, Cluster, Mobility (VMware Vmotion) Microsoft Hyper-V R1 (can be stand alone or role) Microsoft Hyper-V R2 (can be stand alone or role) BIOS (SMBIOS 2.5 or higher) & Operating System boot core limit System scaling using Intel QuickPath Interconnect Fix Pack 1 Kernel-based Virtual Machine (KVM), on RHEV with RHEV-M (Red hat Linux Virtualization Manager) 3.0
Server 2003 R2 (32-bit and 64-bit) **Server 2003 Datacenter** (32-bit and 64-bit)	Service Pack 2	VMware ESX 3.0 - Single Server, Cluster, Mobility (VMware Vmotion) VMware ESX 3.5 - Single Server, Cluster, Mobility (VMware Vmotion) VMware ESXi 3.5 - Single Server, Cluster, Mobility (VMware Vmotion) VMware ESX 4 - Single Server, Cluster, Mobility (VMware Vmotion) VMware ESXi 4 - Single Server, Cluster, Mobility (VMware Vmotion) VMware ESX 4.1 - Single Server, Cluster, Mobility (VMware Vmotion) VMware ESXi 4.1 - Single Server, Cluster, Mobility (VMware Vmotion) VMware vSphere 5 - Single Server, Cluster, Mobility (VMware Vmotion) VMware vSphere 5.1 - Single Server, Cluster, Mobility (VMware Vmotion) Microsoft Hyper-V R1 (can be stand alone or role) Microsoft Hyper-V R2 (can be stand alone or role) BIOS (SMBIOS 2.5 or higher) & Operating System boot core limit (with the exception of XP) System scaling using Intel QuickPath Interconnect Fix Pack 1 Kernel-based Virtual Machine (KVM), on RHEV with RHEV-M (Red hat Linux Virtualization Manager) 3.0
Server 2003 Enterprise Edition (32-bit and 64-bit)	Service Pack 2	VMware ESX 3.0 - Single Server, Cluster, Mobility (VMware Vmotion) VMware ESX 3.5 - Single Server, Cluster, Mobility (VMware Vmotion) VMware ESXi 3.5 - Single Server, Cluster, Mobility (VMware Vmotion) VMware ESX 4 - Single Server, Cluster, Mobility (VMware Vmotion) VMware ESXi 4 - Single Server, Cluster, Mobility (VMware Vmotion) VMware ESX 4.1 - Single Server, Cluster, Mobility (VMware Vmotion) VMware ESXi 4.1 - Single Server, Cluster, Mobility (VMware Vmotion) VMware vSphere 5 - Single Server, Cluster, Mobility (VMware Vmotion) VMware vSphere 5.1 - Single Server, Cluster, Mobility (VMware Vmotion) Microsoft Virtual Server 2005 BIOS (SMBIOS 2.5 or higher) & Operating System boot core limit System scaling using Intel QuickPath Interconnect Fix Pack 1 Kernel-based Virtual Machine (KVM), on RHEV with RHEV-M (Red hat Linux Virtualization Manager) 3.0
Server 2003 Standard Edition (32-bit and 64-bit)	Service Pack 2	
XP Professional	Service Pack 2	

Other software requirements for the agents

Ensure that the corequisite software is installed on the computer where you are installing the agent.

Software deployed together with the agents (automatically)

The 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

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

Note: IBM i The agent does not install Global Security Toolkit - it uses the version that is already part of the system framework.

Table 33. Global Security Toolkit

Operating system	Version	Global Security Toolkit Version
IBM i	V5R3, V5R4, V6R1	6b
Other platforms		7.0.4.14

Common Inventory Technology

It is a component technology used to collect hardware, software, file system, and registry information from systems in a network. It might already be deployed for use by other applications on the target computer so the deployment process checks if the installed version is supported for the License Metric Tool agent. If the installed version is older than recommended, it is upgraded to the supported one.

Partitioning technology prerequisites

Common Inventory Technology enabler

Common Inventory Technology enabler is a script that enables 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.

Important: If you cannot connect to a VM manager, you must run this script on every computer on which there are guest operating systems with License Metric Tool agents deployed on them.

Table 34. 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`
			Other servers
			`enabler/VMWare/linux-ix86`

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

Virtualization tools

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

Table 35. Virtualization tools

Tool	Partitioning technology
VMware Tools (optional)	VMware ESX 3.0 VMware ESX 3.5 VMware ESXi 3.5 VMware ESX 4 VMware ESXi 4
Microsoft Virtual Machine Additions	Microsoft Virtual Server 2005
HPVM package (host operating system) **HPVM-Guest** (guest operating system)	HP Integrity Virtual Machines

Other prerequisites

Table 36. Other agent prerequisites

Required software	Description
lsvpd utility	On POWER® 5+ QCM processors, you need to install the **lsvpd** utility on the target system. The lsvpd utility is provided by IBM for free and it is included in the "IBM Installation Toolkit for Linux" available for download from http://www14.software.ibm.com/webapp/set2/sas/f/lopdiags/installtools/home.html. The latest version of the lsvpd package is also available for download from "Service and productivity tools for Linux on POWER systems" at http://www14.software.ibm.com/webapp/set2/sas/f/lopdiags/
sed, and **grep**	After the installation of the lsvpd utility, you need to initialize the database by issuing the following command: `/etc/init.d/lsvpd start` Sed and grep binary files are required on computers on which agents are to be installed. These binaries are needed during the installation of agents.

Table 36. Other agent prerequisites (continued)

Required software	Description
lsof	AIX Solaris For AIX and Solaris, the dependency scan works only if the **lsof 4.80** diagnostic tool is installed. The default **lsof** installation path is `/usr/sbin/lsof`. If you choose an installation path other than the default, you must issue the `wscancfg -s lsof.bin PATH_TO_LSOF_BINARY` command. For example, for Common Inventory Technology installed in a default location: `/opt/tivoli/cit/bin/wscancfg -s lsof.bin /opt/sbin/lsof` will instruct Common Inventory Technology to use **lsof** located in `/opt/sbin/`. To download **lsof 4.80** visit: • AIX AIX Web Download Pack Programs • Solaris You can download the tool using the link below: lsof 4.80 for Solaris **Tip:** Dependency scans work if the following commands can be executed with the **lsof** you installed: 1. `lsof -i4 -i6 -P -n` (for AIX, Solaris 8 and Solaris 9) 2. `lsof -z -i4 -i6 -P -n` (for Solaris 10 and Solaris 11) Solaris 10 requires the following versions of **lsof** : • Solaris 10 05/08 or higher requires **lsof** 05/08 4.80 • Solaris 10 11/06 with a patch applied to the kernel requires **lsof** 05/08 4.80 • Solaris 10 11/06 or lower requires **lsof** 11/06 4.80
Windows Management Instrumentation (WMI)	Windows *Windows Management Instrumentation* must be enabled on Windows computers in order to run the agent.

VMware and Microsoft virtualization considerations

Both the server and agents can be installed on 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 information, it is impossible to calculate processor value unit (PVU) and systems 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 IBM License Metric Tool.

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 4.0
- VMware ESX Server 3.5
- VMware ESX Server 3.0

On VMware ESX Server 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.

Note: In Windows Server 2008 R2, processor group is a group of logical processors up to the maximum of 64. You can have a maximum of four kernel groups. Hyper-V is not kernel group-aware and does not support more than 64 processors. In a case when Hyper-V is configured and the total number of logical processors exceeds the limit of 64 processors, the CPU will not be recognized correctly.

Disk space requirements

Before deploying the IBM License Metric Tool 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 a message that the agent signature file could not be written to the agent installation folder.

Agent space requirements for AIX

Table 37. License Metric Tool agent space requirements

Operating system	Directory	Space required
AIX, 7.5 GA installation package - **standard installation location**	Agent application directory (default: `/opt/itlm`)	26 MB
	Agent data directory (`/var/itlm`)	29 MB
	Temporary directory (default: `/tmp`)	70 MB
	`Tivoli_Common_Directory``/COD`	10 MB
	Directory for configuration files (default: `/etc`)	under 1 MB
	Common Inventory Technology (default directory: `/opt/tivoli/cit`)	40 MB
	Common Inventory Technology cache files (default: `/opt/tivoli/cit/cache_data/__username`)	about 500 MB 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 60 bytes.

Table 37. License Metric Tool agent space requirements (continued)

Operating system	Directory	Space required
AIX, 7.5 GA installation package - **non-standard installation location**	Agent installation directory - *User Specified Installation Location* (USIL) created with **mkusil** command	58 MB
	Temporary directory (default: /tmp)	70 MB
	Tivoli_Common_Directory/COD	10 MB
	Directory for configuration files (default: /etc)	under 1 MB
	Common Inventory Technology (default directory: /opt/tivoli/cit)	40 MB
	Common Inventory Technology cache files (default: /opt/tivoli/cit/cache_data/__username)	about 500 MB 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 60 bytes.

Space requirements for agents on HP-UX on PA-RISC

Operating system	Directory	Space required
HP-UX on PA-RISC	Agent installation directory (default: /var/itlm)	100 MB
	Temporary directory (default: /tmp)	90 MB
	Tivoli_Common_Directory/COD	10 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)	500 MB 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 60 bytes.

Agent space requirements for HP-UX on Itanium 2 Integrity Server

Operating system	Directory	Space required
HP-UX on Itanium 2 Integrity Server	Agent installation directory (default: `/var/itlm`)	130 MB
	Temporary directory (default: `/tmp`)	120 MB
	`Tivoli_Common_Directory``/COD`	10 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`)	500 MB 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 60 bytes.

Agent space requirements for IBM i

Operating system	Directory	Space required
IBM i (formerly i5/OS™)	Agent installation directory	80 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`)	500 MB 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 60 bytes.

Agent space requirements for Linux x86

Operating system	Directory	Space required
Linux x86	Agent installation directory (default: `/var/itlm`)	40 MB
	Temporary directory (default: `/tmp`)	50 MB
	`Tivoli_Common_Directory``/COD`	10 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`)	500 MB 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 60 bytes.

Agent space requirements for Linux pSeries®

Operating system	Directory	Space required
Linux on Power Systems	Agent installation directory (default: /var/itlm)	40 MB
	Temporary directory (default: /tmp)	50 MB
	Tivoli_Common_Directory/COD	10 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)	500 MB 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 60 bytes.

Agent space requirements for Linux zSeries

Operating system	Directory	Space required
Linux on System z	Agent installation directory (default: /var/itlm)	100 MB
	Temporary directory (default: /tmp)	60 MB
	Tivoli_Common_Directory/COD	10 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)	500 MB 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 60 bytes.

Agent space requirements for Solaris on x86

Operating system	Directory	Space required
Solaris on x86	Agent installation directory (default: /var/itlm)	50 MB
	Temporary directory (default: /tmp)	55 MB
	Tivoli_Common_Directory/COD	10 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)	500 MB 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 60 bytes.

Agent space requirements for Solaris on SPARC

Operating system	Directory	Space required
Solaris on SPARC	Agent installation directory (default: `/var/itlm`)	55 MB
	Temporary directory (default: `/tmp`)	65 MB
	`Tivoli_Common_Directory``/COD`	10 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`)	500 MB 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 60 bytes.

Agent space requirements for Windows

Operating system	Directory	Space required
Windows	Agent installation directory (default: `%WINDIR%/itlm`).	35 MB
	Temporary directory (default: `%TEMP%`)	30 MB
	`Tivoli_Common_Directory``/COD`	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`)	500 MB 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 60 bytes.

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.

The IBM License Metric Tool agent is able to collect 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

License Metric Tool 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 License Metric Tool, 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 and systems calculation for your software installed in High Availability Cluster Multiprocessing environment by excluding one or more software instances.

Support for system scaling using Intel QuickPath Interconnect

IBM License Metric Tool provides support for system scaling using Intel QuickPath Interconnect that enables scalable PVU consumption. The support has been introduced with Fix Pack 1 for IBM License Metric Tool 7.2.2.

IBM System x® has introduced a new technology based on Intel Xeon Nehalem-EX processors and a feature called Intel QuickPath Interconnect. With this technology you can join two computers with a physical link, which increases the capacity of one of the computers. The increased number of cores is reflected in the full capacity of a computer and its PVU value per core.

The table illustrates the change in the capacity and PVU value after 2 computers have been linked with the QuickPath Interconnect link:

Table 38. Change in the capacity and PVU value

Computer A capacity	Computer B capacity	The capacity of both computers linked with QuickPath Interconnect
2 sockets with Intel Xeon (Nehalem-EX) 4 cores with 70 PVU each	2 sockets with Intel Xeon (Nehalem-EX), 4 cores with 70 PVU each	Computer A: 4 sockets and 16 cores with 100 PVU each Computer B: Offline

When you link two computers with the use of QuickPath Interconnect, the reports generated might not provide information about the actual number of cores on both computers. The table illustrates the problem:

Table 39. Cores represented in the report after linking two computers with the use of QuickPath Interconnect

Day	Computer A	Computer B	Report
Day 1: the computers are separated	• 2 sockets • 8 cores • 70 PVU per core • 1 agent with DB2 and WebSphere Application Server installed	• 2 sockets • 8 cores • 70 PVU per core • 1 agent with DB2 installed	

Table 39. Cores represented in the report after linking two computers with the use of QuickPath Interconnect (continued)

Day	Computer A	Computer B	Report
Day 2, 10 a.m.: computer B is connected to computer A with the QuickPath Interconnect link	• 4 sockets • 16 cores • 100 PVU per core • 1 agent with DB2 and WebSphere Application Server installed	Offline from 10 a.m.	The report generated for day 2 lists the following items: • DB2: 24 cores • WebSphere Application Server: 16 cores

There is no technical possibility to automatically detect the problem and exclude computer B from the report for day 2. The situation might result in overcharging. To prevent the problem, you can either disable the agent the day before you connect the computers (UTC time), or exclude the miscalculated product instances on the agent on computer B from the report.

To disable the agent:

1. Shut down or uninstall the agent on computer B one day before the connection date.
2. Remove the agent from the License Metric Tool Web user interface.
3. Connect the computers the next day.

To exclude the miscalculated product instances on the agent on computer B from the report:

1. Close the current audit report the day before the connection date.
2. Connect the computers the next day.
3. Exclude the miscalculated product instances on agent B from the report.

Supported national languages for IBM i agents

You must install one of the supported languages as your primary or secondary language on the IBM i node.

Installed languages on IBM i		
	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

Installed languages on IBM i		
	2987	Traditional Chinese
	2989	Simplified Chinese
	2923	Dutch
	2912	Croatian
	2911	Slovenian

Agent preinstallation steps

Depending on your software and the security level that you selected, you must perform several tasks before you install the agents.

About this task

Important:

- The agent installer does not allow you to use non-Latin characters when specifying path names and the scan group name. Examples: the agent installation path, Common Inventory Technology installation path, or the temporary folder for the agent. 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 during installation. Next, reassign it to the target scan group after the installation finishes.
- The agent response file and log file names cannot contain two byte characters.
- To install and run agents, you must have root (UNIX) or Administrator (Windows) authority. This requirement is mandatory because each agent is registered as system service.
- You can install agents regardless of whether the License Metric Tool server is running.
- AIX Solaris For AIX and Solaris, the dependency scan works only when the lsof 4.80 diagnostic tool is installed.

Procedure

1. Gather the following information:
   - The administration server address and the port number that agents are to use.
   - The level of security that was configured for the server. At the server command line, issue the command **`getserverconf -k agentToServerSecurityLevel`**.
   - The proxy port and address if you want the agent to use a proxy server for communication with the server.
2. .Specify agent installation packages
3. Prepare agent installers if you have downloaded the installation images from Passport Advantage (or copied from the DVD).
4. If the unzip utility is not installed on your AIX server, download, install, and use the program to be able to extract .zip installer files.
5. Optional: Enable **medium** or **maximum** security level depending on the choice you made while installing the administration server.

For medium security level	For maximum security level
go to the topic “Enable medium security” in the “Security” section of the information center.	go to the topic “Enable maximum security” in the “Security” section of the information center.

6. UNIX If you want to install agents on a shared file system, ensure that you exported and mounted the remote directory. Change the permissions on mounted directories and files by using the **chown**, and **chmod** commands.
7. Configure any firewalls between the agent and server computers to allow the agent access to the server.
8. Optional: Create scan groups that you can use later for scheduling software scans, so that 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.
9. Windows If Windows Terminal Server is installed on the computer on which you want to run the setup file, ensure that the computer is in **installation** mode when the setup file is launched. Do the same if you are accessing another computer with Windows Terminal Services.
   a. Issue the command **change user /install** from a Windows command line to change into the installation mode manually.
   b. After running the setup file, return to execute mode by running **change user /execute**.
10. If you want to use your own tools to install agents in bulk, ensure that the value in the **current_working_directory** parameter is not set to **null** when running a new process on a target computer.
11. If you are installing the agent in a partitioned environment with a VMware or Microsoft Virtual Server virtualization technology, ensure that the machine can be connected to a virtual machine manager.

    If one of your computers cannot be connected to a VM manager, run the Common Inventory Technology enabler.
12. Red Hat Set SELinux to disabled because the permissive SELinux setting is too restrictive for agent installation.
13. Set up a proxy server in your infrastructure so that the agent-server data is able to pass through network firewalls.
14. AIX Create a *User Specified Installation Location* (USIL) with the **mkusil** command if you want to install the agents in a non-standard location.
15. Windows Enable *Windows Management Instrumentation* on Windows computers in order to run the agent after the installation.

Extracting files from .zip packages on AIX

If you do not have unzip installed on your AIX server, download, install and use the program to be able to extract files from the .zip packages.

Before you begin

- Download and install the **unzip** program (`unzip-program_version.aix_version.ppc.rpm`) available on IBM AIX Toolbox download information website.

About this task

The following License Metric Tool installers are provided in the `.zip` format on the AIX platform:

- `ILMT-server-7.5-aix-ppc64.zip`
- `ILMT-TAD4D-patchtool-7.5-aix-ppc64.zip`
- `ILMT-TAD4D-agent-7.5-spb-all.zip`

Procedure

1. Log on to the AIX server.
2. To uncompress the server installer, issue the following command: **unzip** *installer_filename* To list the contents of the compressed file, issue **unzip -l** *installer_filename*.

Running Common Inventory Technology enabler

If you cannot define VM Managers, you must use Common Inventory Technology enabler instead. It is required because License Metric Tool server has to gather vital information about virtual manager hierarchy. Before installing License Metric Tool agent on a virtual machine hosted by either Microsoft Virtual Server or a VMware server, you must install and run CIT enabler on the appropriate host computer.

Before you begin

Important: Running the Common Inventory Technology enabler is not required when a given agent is managed by a VM Manager (including IBM WebSphere CloudBurst® Appliance).

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 operating systems for agents" on page 80.

About this task

Common Inventory Technology (CIT)

It is a component technology used to collect hardware, software, file system, and registry information from systems in a network. There are three types of scans performed by the agent using the CIT component:

- Software scans detect installed software products. (Registry scans return information on installed software products and patches by scanning the registries.)
- The software use scanner monitors applications running at a given moment.
- Hardware scans return information on the hardware characteristics of the scanned system.

Common Inventory Technology enabler

Common Inventory Technology provides an enabler to export correct data to the guest systems so that CIT instances installed on each operating system partition can discover and return correct data. CIT enabler is a script that allows Common Inventory Technology to obtain information about the VMware or Microsoft Virtual Server virtualization environment. The enabler is installed on the computer which hosts the guest operating systems, and it stores the correct hardware information on the guest operating systems.

Attention: You must run CIT enabler on host computers that have guest operating systems installed, on which you intend to install License Metric Tool agents. You must run the enabler script on the host system first, before installing the IBM License Metric Tool agent, and again after every reboot or VM configuration change.

From version 2.6, fix pack 2, Common Inventory Technology has been enhanced with a detailed report from its execution and some additional features:

- A new **-r** option to retrieve.sh generates a report in the `./en_report.txt` file. The report contains the result of the enabler execution for each Virtual Machine. The report will also be generated if `retrieve.sh` is executed with the **-v** option.
- Running `wenvmw.sh` with the **-v** option generates a report file by default.
- When the enabler fails to transfer the data successfully onto a Virtual Machine, the report contains the exact command that you can copy and run on the Virtual Machine.
- A new **-vm** option to retrieve.sh forces the enabler to run only for this particular Virtual Machine.

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 virtual machines.

Procedure

1. Find the files for your platform and partitioning technology in the `enabler` directory on the installation DVD, or in the .zip and .tar.gz files for your platform if you downloaded the enabler files from the IBM Passport Advantage website. Copy the files for your environment to a directory on the host virtual server system. Copy all files into the same directory. On UNIX systems, remember to keep file attributes (execute attribute).

   Note: To enable the installation on both Windows and Linux operating systems, the files are provided in the .zip and .tar.gz formats. The following files are required on each host:

Table 40. Files required to run the Common Inventory Technology enabler

Partitioning technology	Required files
VMware host	Windows: `wenvmw.exe`, `cpuid.exe`, `retrieve.pl`
	Linux: `wenvmw.sh`, `cpuid`, `dispatcher`, `retrieve.pl`
Microsoft Virtual Server host	Windows: `wenmsvs.exe`, `cpuid.exe`

2. Run the enabler script with 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 script.
3. Check the logs to see whether the script was run successfully.

What to do next

Now, you can install the agent on the guest system.

Disabling SELinux when installing the agent on Red Hat 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.

Procedure

1. Open the `/etc/selinux/config` file.
2. Set the **SELINUX** parameter to `disabled`.
3. Restart your machine.

Setting up a proxy server

You can configure a proxy server in your infrastructure so that the agent-server data is able to pass through network firewalls.

Before you begin

- You must have the following operating system privileges:
  - Windows Administrator
  - UNIX root
- You need to have an IBM HTTP Server installed and running on a dedicate server computer. For details on how to install IBM HTTP Server refer to WebSphere Application Server information center .

- You require the IBM HTTP Server administrator user name and password.

About this task

To define a proxy server for communications between agents and the License Metric Tool server, complete the following steps:

Procedure

1. Stop the IBM HTTP Server by issuing the following command (or option in the **Start** menu):
   - AIX `/usr/IBMIHS/bin/ apachectl stop`
   - UNIX `/opt/IBMIHS/bin/ apachectl stop`
   - Windows From the **Start menu**, select **IBM HTTP server** and then **Stop HTTP Server**.
2. On the HTTP server edit the `httpd.conf` file. Find the following section and uncomment the lines in bold:

```
# Example:
# LoadModule foo_module modules/mod_foo.so
LoadModule access_module modules/mod_access.so
LoadModule auth_module modules/mod_auth.so
#LoadModule auth_anon_module modules/mod_auth_anon.so
#LoadModule auth_dbm_module modules/mod_auth_dbm.so
LoadModule include_module modules/mod_include.so
LoadModule log_config_module modules/mod_log_config.so
LoadModule env_module modules/mod_env.so
#LoadModule mime_magic_module modules/mod_mime_magic.so
#LoadModule cern_meta_module modules/mod_cern_meta.so
#LoadModule expires_module modules/mod_expires.so
#LoadModule headers_module modules/mod_headers.so
#LoadModule usertrack_module modules/mod_usertrack.so
LoadModule unique_id_module modules/mod_unique_id.so
LoadModule setenvif_module modules/mod_setenvif.so
LoadModule proxy_module modules/mod_proxy.so
#LoadModule proxy_connect_module modules/mod_proxy_connect.so
#LoadModule proxy_ftp_module modules/mod_proxy_ftp.so
LoadModule proxy_http_module modules/mod_proxy_http.so
LoadModule mime_module modules/mod_mime.so
#LoadModule dav_module modules/mod_dav.so
LoadModule autoindex_module modules/mod_autoindex.so
#LoadModule asis_module modules/mod_asis.so
#LoadModule info_module modules/mod_info.so
LoadModule cgid_module modules/mod_cgid.so
#LoadModule dav_fs_module modules/mod_dav_fs.so
#LoadModule vhost_alias_module modules/mod_vhost_alias.so
LoadModule dir_module modules/mod_dir.so
#LoadModule imap_module modules/mod_imap.so
LoadModule actions_module modules/mod_actions.so
#LoadModule speling_module modules/mod_speling.so
LoadModule userdir_module modules/mod_userdir.so
LoadModule alias_module modules/mod_alias.so
#LoadModule rewrite_module modules/mod_rewrite.so
#LoadModule deflate_module modules/mod_deflate.so
```

3. In the section `LoadModule`, add the following lines:

```
<IfModule mod_proxy.c>
ProxyRequests Off
ProxyPass / http://lmt_server_IP_address:port/
ProxyPassReverse / http://lmt_server_IP_address:port/
</IfModule>
```

4. Open the `httpd.conf` file, search for the line `Listen 80` and change it to `Listen 9988`. 9988 is the default port used for agent to server communication. Use the appropriate value if you are not using the default one.
5. Start the server by issuing the following command (or option in the **Start** menu):
   - AIX `/usr/IBMIHS/bin/ apachectl start`
   - UNIX `/opt/IBMIHS/bin/ apachectl start`
   - Windows From the **Start menu**, select **IBM HTTP server** and then **Start HTTP Server**.

Results

Now agents can access the server using the IP address of the IBM HTTP Server. You can verify that by using the following URL: `http://`*`http_server_ip_address`*`:9988/msghandler/service`

Performing agent security-related tasks

Perform a few security tasks in order to enable secure communication. These tasks must be done before you install agents in your infrastructure.

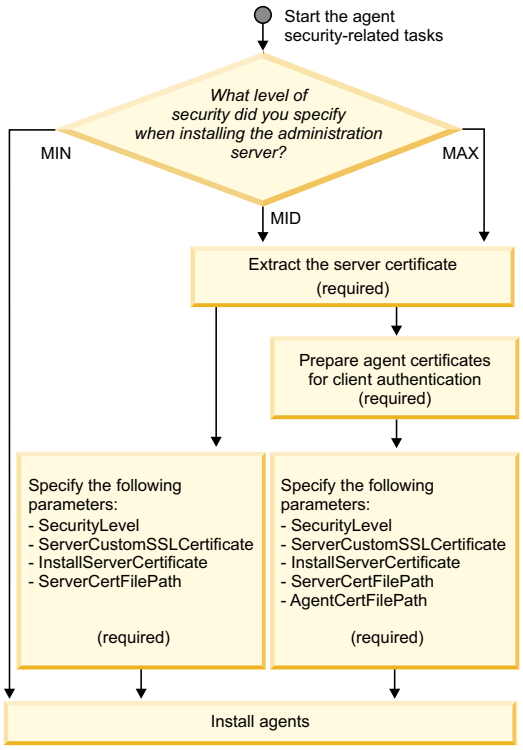
Before you begin

If you defined **medium** or **maximum** security level during the installation of the administration server, you must prepare the packages that are to be distributed before you do the agent security-related tasks. For more information, go to “Agent preinstallation steps” on page 100.

About this task

The following diagram shows 2 tasks:

- creating agent certificates, and
- creating administration server certificates



1. Required (medium or maximum level) Extract server certificate

   Personal certificate containers comprise a private key and a public key. You can extract the public key, called the signer certificate, to a file, then import the certificate into another keystore.

   Note: The server certificate file must be named `cert.arm`. If a different name is used, the response file or shell installer will accept it but a GSKit error will be reported.
2. Required (maximum level) Prepare 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 certificate contains a unique agent ID and a public key.
3. Required: Specify security parameters in response files or agent installation software package blocks, or configure UNIX shell installer before installing agents.

   The following parameters must be specified before the installation of agents:

   - **`SecurityLevel`**
   - **`ServerCustomSSLCertificate`**
   - **`InstallServerCertificate`**
   - **`ServerCertFilePath`**
   - **`AgentCertFilePath`** (maximum security only)

After you have completed these tasks, you can proceed to installing agents using one (or more) of the available methods (tools):

- Tivoli Configuration Manager
- native installers
- Windows Logon Scripts
- shell installers (UNIX platforms only)

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 certificate contains a unique agent ID and a public key.

Before you begin

This procedure is only relevant if you are using the maximum security level. To perform this task, ensure that you have a certificate issued by a certificate authority, either a private or public one. For medium security, continue from: deploying agents and certificates.

To perform the task, you must have the following operating system privileges:

- Windows Administrator
- UNIX root

Procedure

1. Access the License Metric Tool command line interface.

2. Assess how many agents you are planning to deploy with maximum security, then issue the following command:

   generateAgentId -d *output_dir_name* **-p** *password* **-n** *number_of_IDs*

   output_dir_name
   The name of the output directory

   password
   Password that is used to encrypt key files

   number_of_IDs
   The number of IDs that you want to create (It equals the number of agents)

   Example: UNIX Linux `generateAgentId -d /root/agents -p slmtest -n 1` It will create the following directories within the output directory you specify:

   - `csr`: contains a Certificate Signing Request (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:

   a. Get the request signed by a certificate authority to form an agent certificate:

openssl x509 -req -days *number_of_days* **-in** *full_path_to_CSR* **-CA** *path_to_ca_cert* **-CAkey** *path_to_ca_key* **-set_serial** *serial_no* **-out** *path_to_agent_cert*

   where:

   number_of_days
   The number of days the certificate is to be valid

   full_path_to_CSR
   The full path to the Certificate Signing Request

   path_to_ca_cert
   The path to CA certificate file

   path_to_ca_key
   is the path to the agent certificate file

   serial_number
   is the certificate serial number that is to be used

   path_to_agent_cert
   is the path to the agent certificate file

   Example: UNIX Linux `openssl x509 -req -days 7300 -in agents/csr/1_1.arm -CA ca/ca.crt -CAkey ca/ca.key -set_serial 01 -out agents/1_1.crt`

   b. Produce a PKCS12 keystore (`.p12`) file, protected by a password, that contains the agent certificate, private key, and CA certificate with the chain of certificates up to the root CA certificate.

openssl pkcs12 -export -in *path_to_agent_cert* **-inkey** *agent_private_key* **-certfile** *path_to_ca_cert* **-name "itlm agent certificate" -out** *path_to_PKCS12*

   where

path_to_agent_cert
is the path to the agent certificate

agent_private_key
Full path to agent private key

path_to_ca_cert
Full path to CA certificate file

path_to_PKCS12
Full path to PKCS12 keystore

Example: UNIX Linux `openssl pkcs12 -export -in agents/1_1.crt -inkey agents/privkey/1_1.key -certfile ca/ca.crt -name "itlm agent certificate" -out agents/1_1.p12`

Friendly name must be set to **itlm agent certificate**.

c. Import the CA certificate to the Signer Certificate section of the ILMT truststore on the server. **SSL certificate and key management** > **Key stores and certificates** > **ILMTtruststore** > **Signer certificates** > **Add**

4. From the License Metric Tool CLI, issue a command to convert the keystore file to a format supported by the security software used by the agent: **convertcertificate**

convertcertificate -d *output_dir_name* **-p** *password* **-op** *output_password*

Example:

- UNIX Linux `convertcertificate -d /root/agents -p slmtest -op slmtest`
- IBM i `convertcertificate -d /root/agents -p slmtest -op slmtest -os400 y`

where

output_password
is the required password: **slmtest**

Note: For agents on IBM i, the **convertcertificate** command converts the files found in the specified directory to the keystore format and version supported by IBM i and stores them.

5. If you did not install the following fix packs:
   - 19 or higher for WebSphere Application Server

   Or:
   - Java SDK for WebSphere Application Server, containing IBM Java 6.0 SR10

   perform the following steps for each agent:

   a. Set the path to the Global Security Toolkit libraries by issuing the commands:
      - Windows `set PATH=%PATH%;agent_dir\gskit\lib`
        For example: `set PATH=%PATH%;c:\windows\itlm\gskit\lib`
      - AIX Linux Solaris `export LD_LIBRARY_PATH=agent_dir/gskit/lib`
        For example: `export LD_LIBRARY_PATH=/opt/itlm/gskit/lib`
      - HP-UX `export SHLIB_PATH=agent_dir/gskit/lib`
        For example: `export SHLIB_PATH=/var/itlm/gskit/lib`

   b. Issue the following command:

GSK7CAPICMD_ABSOLUTE_PATH -cert -export -db agentID.kdb -pw slmtest -target agentID_fixed.kdb -target_pw slmtest

where GSK7CAPICMD_ABSOLUTE_PATH is:

- Windows *agent_dir*\gskit\bin\gsk7capicmd.exe
- UNIX agent_dir/gskit/bin/gsk7capicmd

For example:

- Windows
  c:\Windows\itlm\gskit\bin\gsk7capicmd.exe -cert -export -db agentID.kdb -pw slmtest -target agentID_fixed.kdb -target_pw slmtest
- UNIX
  /opt/itlm/gskit/bin/gsk7capicmd -cert -export -db agentID.kdb -pw slmtest -target agentID_fixed.kdb -target_pw slmtest

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

Installing agents using native installers

Installation scripts or wizards are available for all supported platforms.

About this task

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. Use the response file 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.

Note: When you decided to install an agent on the computer where the stand-alone scan had been run before, the list of agents will show two records referring to the same computer. To fix this situation, you have to manually remove the agent that belongs to the stand-alone scan group. For more information, see Removing agents.

Installing agents on AIX using native installers

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

Before you begin

- Ensure that the computers on which you plan to install agents meet all requirements. See: Planning the installation of agents.
- You must have root privileges.
- 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 a WPAR.
- You must ensure that agent is installed on WPAR host (in most cases it is an LPAR).

About this task

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 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. The `tlmagent.ini` file is located in the `/etc` directory.

The default agent installation directories are `/var/itlm` (data directory containing cache) and `/opt/itlm` (program directory containing executable files), and you cannot change these locations. You can also install the agent in a *User Specified Installation Location*.

If you install Common Inventory Technology in a workload partition in default location (`/opt`), you will have all the binary files shared with the 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 binary files 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.

Note: The agent installation pack does not check for the disk space available for the Common Inventory Technology installation.

Procedure

1. Log on to the computer where you want to install the agent as a user with administrative rights.
2. Copy the compressed agent installation package `CI27RML.tar.gz` to a temporary directory on the agent computer - either from a DVD or from a directory where you store the files downloaded from Passport Advantage. The package contains agent native installers for all supported platforms. This is needed because the operating system generates the `.toc` file before starting the installation of the fileset.
3. Open the system command line and change to the directory where you store the file.
4. Extract the files 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 have two files:

   - `ILMT-TAD4D-agent-7.5-aix-ppc`
   - `response_file.txt`

5. Optional: Update the parameters in the `response_file.txt` file. Edit this template response file to change the necessary parameters, for example the IP address of the administration server. Perform the following steps:
   a. Edit the response file to customize its parameters to your situation.
   b. 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: `LMT_RESPONSE_FILE_PATH=/tmp/my_response_file.txt`

   If no environment variable is 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.

   Note: If your AIX platform is partitioned using the WPAR partitioning technology, and you want to install an agent using the response file, copy the `response_file.txt` file to the `/etc` directory on every WPAR guest.
6. To install the agent, issue the following command from the directory where you have extracted the installer:

   ```
   installp -acgXd ILMT-TAD4D-agent-7.5-aix-ppc
   ILMT-TAD4D-agent
   ```

   In WPAR environments, issue one of the following commands:
   - In WPAR:

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

     Before you run the command, ensure that the agent is installed on the WPAR host (in most cases it is an LPAR).
   - In LPAR:

     ```
     syncwpar WPAR_name
     ```

     This command installs the agent by synchronizing a WPAR with the LPAR. To learn the name of the WPAR, issue the command **lswpar**

     The WPAR installation path must be the same as the one for LPAR.

   To install the agent in a directory different from the default one, choose the installation procedure that is suitable for your version of AIX and the version of License Metric Tool interim fix that you are using:

	AIX 5.3 and lower	**AIX 5.3.061 and higher**
Interim fix 5 and lower	Use the `ILMT_INSTALL_PATH` environment variable	Use *User Specified Installation Location* (USIL)
Interim fix 6 and higher	Installation in custom location is not available	Use *User Specified Installation Location* (USIL)

   - For installations that support the use of the `ILMT_INSTALL_PATH` environment variable, set the variable to point to your custom location:

     ```
     export ILMT_INSTALL_PATH=PATH_TO_DESIRED_LOCATION
     ```
   - For installations that support the use of the relocation mechanism that is based on the *User Specified Installation Location* (USIL), perform the following steps:
     a. Create the *custom_location* directory:

        ```
        mkdir -p /custom_location
        ```
     b. Make the directory your *User Specified Installation Location* (USIL):

        ```
        mkusil -R /custom_location
        ```
     c. Install the agent in this location:

```
installp -R /custom_location -acgXd full_path_to_the_installation_package_dir ILMT-TAD4D-
ILMT-TAD4D-agent
```

The agent is installed in */custom_location*/opt/itlm and */custom_location*/var/itlm folders.

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

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

   The `tlmagent.ini` file is located in the `/etc` directory.
   c. Start the agent using the `/usr/bin/startsrc -s tlmagent` command.
8. If you have installed an agent on a logical partition (LPAR) on an AIX 5.2 host that is partitioned using workload partitions (WPARs), you must provide the core allocation for the partition into a configuration file. To do that, edit the `tlmsubcapacity.cfg` file that is located in the /etc directory and add the following line: `NodeCapacityInCores=<total_number_of_cores>`. After you save the file, the agent will use the value as the node capacity so that the aggregated server capacity can be reported correctly.

What to do next

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.

Installing agents on HP-UX using native installers

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

Before you begin

- Ensure that the computers on which you plan to install agents meet all necessary requirements. See: *Agent hardware and software requirements*.
- You must have root privileges.

About this task

Note: You should first install an agent on a HPVM (HP Integrity Virtual Machines) host in order to install the agent in a HPVM guest operating system.

The default agent installation directory is `/var/itlm`. To install the agent in a different directory, specify the *INSTALL_PATH* variable when you run the command described in point 5.

The agent installation pack does not check for the disk space available for the Common Inventory Technology installation.

Procedure

1. Log on to the computer where you want to install the agent as a user with administrative rights.
2. Copy the compressed agent installation package `CI27RML.tar.gz` to a temporary directory on the agent computer - either from a DVD or from a directory where

you store the files downloaded from Passport Advantage. The package contains agent native installers for all supported platforms.

3. Open the system command line and navigate to the directory where you store the compressed package.
4. Extract the files 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-7.5-hpux`
   - `response_file.txt`
5. `response_file.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(r) agents installation response file* for more information. 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.
6. To install the agent enter the following command:

```
swinstall -s ABSOLUTE_PATH_TO_INSTALLER_FILE/ILMT-TAD4D-agent-7.5-hpux ILMT-TAD4D-agent:/INSTALL_PATH
```

   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.
7. 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.

What to do next

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 computer, 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 start the agent using the `tlmagent -g` command.

Note: The `tlmagent.ini` file is located in the `/etc` directory.

Installing agents on IBM i using native installers

You can install agents on the IBM i platform using the **RSTLICPGM** command.

Before you begin

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

About this task

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 i 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.

The default agent installation directory is `/QIBM/ProdData/QITLM`. It is not possible to change the default installation path.

Note: The agent installation pack does not check for the disk space available for the Common Inventory Technology installation.

Procedure

1. If you downloaded the files from Passport Advantage, extract the installation package on a Windows computer. For example:

   ```
   unzip 7.5.0-TIV-ILMT-TAD4D-IF0002-agent-i5os.zip
   Archive:  7.5.0-TIV-ILMT-TAD4D-IF0002-agent-i5os.zip
   inflating: ILMT-TAD4D-agent-7.5.0.2-i5os.savf
   inflating: os400_agent.txt
   ```

2. Create the SAVF file on the target IBM i computer and upload the agent installer:

   a. Enter the **CRTSAVF FILE***obj_name* command to create a save file:

      ```
      CRTSAVF FILE(LMTAGNT)
      RESULT: File LMTAGNT created in library QGPL.
      ```

      The *obj_name* can be up to 10 characters long. By default, the file is created in QGPL library

   b. Upload the SAVF file using FTP, for example:

      ```
      ftp> cd QGPL
      ftp> bin
      200 Representation type is binary IMAGE.
      ftp> put ILMT-TAD4D-agent-7.5.0.2-i5os.savf LMTAGNT
      200 PORT subcommand request successful.
      150 Sending file to member LMTAGNT in file LMTAGNT in library QGPL.
      226 File transfer completed successfully.
      61877376 bytes sent in 3.617 seconds (1.671e+04 Kbytes/s)
      local: ILMT-TAD4D-agent-7.5.0.2-i5os.savf remote: LMTAGNT
      ftp>
      ```

3. `os400_agent.txt` is a template response file. If you want to install the agent with the response file, update the parameters in the file. The server address (**MessageHandlerAddress**) is a mandatory parameter. See "IBM i agent installation response file" on page 142 for more information. To use the same response file to install agents on other systems with the same configuration, copy the file to the `/tmp/itlm` directory on the target computer. Use a new FTP session, for example:

   ```
   ftp> bin
   200 Representation type is binary IMAGE.
   ftp> cd /tmp/itlm
   250-NAMEFMT set to 1.
   250 "/tmp/itlm" is current directory.
   ftp> bin
   200 Representation type is binary IMAGE.
   ftp> put os400_agent.txt
   200 PORT subcommand request successful.
   150 Sending file to /tmp/itlm/os400_agent.txt
   ```

```
226 File transfer completed successfully.
5736 bytes sent in 0.1626 seconds (34.45 Kbytes/s)
local: os400_agent.txt remote: os400_agent.txt
ftp>
```

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)
   SAVF(LIBRARY_WHERE_THE_SAVF_FILE_IS_PLACED/NAME_OF_THE_SAVF)
   ```

   For example:

   ```
   RSTLICPGM LICPGM(1IBMTLM) DEV(*SAVF)  SAVF(QGPL/LMTAGNT)
   ```

   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 IBM i 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`:

   ```
   EDTF '/qibm/userdata/qitlm/conf/tlmagent.ini'
   ```

   Go to:

   ```
   # Preferred Server
   # (Reloadable: No)
   server = LMT_SERVER_NAME
   ```
8. Start the agent using the `strtcpsvr server(*itlmagent)` command.
9. 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.

   Note: To run the Japanese language version of the agent, the CCSID of the job must be 939 (5035) rather than 930 (5026) because agent uses lowercase English characters.

What to do next

After installing the agent with the security level of communication between the agent and the server set to *medium* or *maximum*, it is recommended that you manually clean the agent certificate store using Digital Certificate Manager. For more information, see “Communication security levels” and “Configuring secure communication”.

Installing agents on Linux using native installers

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

Before you begin

- Ensure that the computers on which you plan to install agents meet all necessary requirements. See: “Planning the installation of agents” on page 80.
- You must have root privileges.

About this task

The default agent installation directory is `/var/itlm`. To install the agent in a different directory, run the appropriate command as described in step 5.

Note: The agent installation pack does not check for the disk space available for the Common Inventory Technology installation.

Procedure

1. Log on to the computer where you want to install the agent as a user with administrative rights.
2. Copy the compressed agent installation package `CI27RML.tar.gz` to a temporary directory on the agent computer - either from a DVD or from a directory where you store the files downloaded from Passport Advantage. The package contains agent native installers for all supported platforms.
3. Open a system command prompt and navigate to the directory where you store the file.
4. 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-7.5-linux-x86.rpm` (Linux x86), or
   - `ILMT-TAD4D-agent-7.5-linux-ppc.rpm` (Linux for IBM Power Systems), and
   - `response_file.txt`
5. `response_file.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 139 for more information.
   - 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 copy the response file to the `/etc` directory.
6. Enter the following command:

   ```
   rpm -Uvh ILMT-TAD4D-agent-7.5-linux-x86.rpm
   ```

   or

   ```
   rpm -Uvh ILMT-TAD4D-agent-7.5-linux-ppc.rpm
   ```

   If you want to install the agent in a directory different than the default one, enter the following command:

   `rpm -Uvh ILMT-TAD4D-agent-7.5-linux-x86.rpm --prefix` *`full_installation_path`*

   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.
7. 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.

What to do next

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 computer, use the `tlmagent -e` command to stop the agent, and edit the server location parameter in the `tlmagent.ini` file:

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

Then, start the agent using the `tlmagent -g` command.

Note: The `tlmagent.ini` file is located in the `/etc` directory.

Installing agents on Linux on System z

You can install agents on Linux on System z platform using the **rpm** command.

Before you begin

- Ensure that the computers on which you plan to install agents meet all necessary requirements. See: *Agent hardware and software requirements*.
- You must have root privileges.

About this task

The default agent installation directory is `/var/itlm`. To install the agent in a different directory, run the appropriate command described in point 6.

Note: The agent installation pack does not check for the disk space available for the Common Inventory Technology installation.

Procedure

1. Log on to the computer where you want to install the agent as a user with administrative rights.
2. Copy the compressed agent installation package `CI27RML.tar.gz` to a temporary directory on the agent computer - either from a DVD or from a directory where you store the files downloaded from Passport Advantage. The package contains agent native installers for all supported platforms.
3. Open the system command line and navigate to the directory where you store the installer.
4. 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-7.5-linux-s390.rpm` (Linux on System z), and
   - `response_file.txt`
5. To install the agent, you need to update the parameters in the response file and copy it to the `etc` directory. `response_file.txt` is a template response file. See *UNIX(r) agents installation response file* for more information.

   Important: 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.

6. Use the response file to set the values in the following parameters:

   `MachineType`
   This is a new parameter introduced in IBM License Metric Tool 7.2.1. The possible values are z9® or z10™ (Specify z10 if you are installing the agent on a server computer with the z196 or z114 processor).

   `ProcessorType`
   Provide value CP if your Linux image is running on CP processors and IFL if the image is running on IFL processors.

   `SharedPoolCapacity`
   This is the number of all processors of a given type (CP or IFL) on the physical machine running in shared mode. Specify 0 if LPAR is using only dedicated processors.

   `SystemActiveProcessors`
   If the Linux on System z 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.

   `MessageHandlerAddress`
   Specify the hostname or IP address of the IBM License Metric Tool server. Message handler is a server component which manages incoming and outgoing agent data.

   Note: If you do not set the **`MessageHandlerAddress`** parameter, the agent 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, and edit the server location parameter in the `tlmagent.ini` file located in the `/etc` directory:

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

   Then, start the agent using the `tlmagent -g` command.

   If no values are specified, the installation will fail.

7. Enter the following command:

   ```
   rpm -Uvh ILMT-TAD4D-agent-7.5-linux-s390.rpm
   ```

   To install the agent in a directory different from the default one, enter:

   ```
   rpm -Uvh ILMT-TAD4D-agent-7.5-linux-s390.rpm --prefix full_installation_path
   ```

   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.

8. 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.

Installing agents on Solaris using native installers

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

Before you begin

- Ensure that the computers on which you plan to install agents meet all requirements. See: "Planning the installation of agents" on page 80.
- You must have root privileges.

About this task

The default agent installation directory is `/var/itlm`. To install the agent in a different directory, specify the **AgentInstallPath** parameter in the response file.

Note:

1. If you are installing agents on a Solaris 10 platform that is partitioned using the Containers partitioning technology, you must first install the agent in the global zone. The agent will automatically be installed also in all existing and future local zones. On a Solaris 11 platform, you must install the agent in the global zone and in every local zone separately.
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).
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.
4. The agent installation pack does not check for the disk space available for the Common Inventory Technology installation.
5. Make sure that the console width is set to a maximum of 168 columns.

If you are installing agents on a Solaris platform that is partitioned using Oracle VM Server for SPARC technology (formerly LDOM - Logical Domains), the agent will stay in 'Incomplete' status until the agent from Global Zone on Control Domain is plugged into the server. In Logical Domains environment, agents are not able to entirely determine the underlying virtualization hierarchy. Only the agent in Global Zone on Control Domain knows about the physical computer and all other Guest Domains.

Procedure

1. Log on to the computer where you want to install the agent as a user with administrative rights.
2. Copy the compressed agent installation package `CI27RML.tar.gz` to a temporary directory on the agent computer - either from a DVD or from a directory where you store the files downloaded from Passport Advantage. The package contains agent native installers for all supported platforms.
3. Extract the installer files 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, there should be four files:

   - `ILMT-TAD4D-agent-7.5-solaris-x86_64` (Solaris on EM64T and AMD 64), or

- `ILMT-TAD4D-agent-7.5-solaris-sparc32` (Solaris on SPARC, 32–bit), or
- `ILMT-TAD4D-agent-7.5-solaris-sparc64` (Solaris on SPARC, 64–bit), and
- `response_file.txt`, and
- `update_contents.sh`, and
- `installer_tarball_`*`file_name`*`.tar`

4. `response_file.txt` is a template response file. If you want to install the agent with the response file, update the parameters in the file and copy it to the `/etc` directory. See "UNIX agents installation response file" on page 139 for more information.
5. Install the agent by running the command:

   ```
   pkgadd -d ILMT-TAD4D-agent-7.5-solaris-platform ILMT-TAD4D-agent
   ```

   Important: If you are installing agents on a Solaris 11 platform that is partitioned using the Containers partitioning technology, you must run the installation command on every zone separately.
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 user interface 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.

What to do next

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

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

  Then, start the agent using the `tlmagent -g` command.

  Note: The `tlmagent.ini` file is in the `/etc` directory.
-

  Important: If you want to enable self-update for an agent installed on bare metal Solaris 10, you must restart the agent after 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.

Before you begin

Ensure that the computers on which you plan to install agents meet all necessary requirements. See: "Planning the installation of agents" on page 80.

About this task

The default agent installation directory is `Windows\itlm`. If you want to install the agent in a different directory, specify the **`Agent destination folder`** parameter as described in step 6.

Note:

1. The IBM License Metric Tool installer does not support file names with double-byte characters including log file names and response file names.
2. The agent installer does not check for the disk space available for the Common Inventory Technology installation.

Installing agents interactively

About this task

If you decided to install interactively, use 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 a response file which you will later use to install agents on other Windows computers.

Procedure

1. Log on to the computer where you want to install the agent as a user with administrative rights.
2. Copy the compressed agent installation package `CI27RML.tar.gz` to a temporary directory on the agent computer - either from a DVD or from a directory where you store the files downloaded from Passport Advantage. The package contains agent native installers for all supported platforms.
3. Extract the installer files using a utility that supports the `tar`, and `gz` formats. The main file `setup.exe` is located in directory *`temp_dir`*`\ILMT-TAD4D-agent-7.5-windows-x86`.
4. Click **setup.exe** to launch the installation wizard.
5. Select the language version that you want to install and click **Next**.
6. A welcome panel opens. Click **Next**.
7. 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.Click **Next**.
8. Specify the agent parameters:

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

   Note: It is impossible to install agents in 64-bit Windows directory `Program Files`. If you install the agent in `c:\Program Files` on 64-bit Windows, this path will be changed to the 32-bit directory `c:\program files(x86)`.

   Agent temporary folder
   The folder in which the agent installer stores files during the installation process

Common Inventory Technology destination folder
The folder in which the Common Inventory Technology files will be installed.

Click **Next**.

9. 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 list.

HTTP To use nonsecure 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 nonsecure 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 License Metric Tool information center.

Use FIPS level of encryption
Selecting this option enables the 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 **Server certificate file** group box in the lower part of the panel and enables the installation of the security certificate (not applicable if you choose minimum security option).

Under the Server certificate file specify the following:

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 server 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.

In the Agent certificate file group box, specify the following:

Install agent certificate file
Selecting the Install agent certificate file check box allows you to specify the path to the certificate file below.

Click **Next**.

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

    Under Proxy Settings, specify the following:

    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**.

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

    Scan group
    The name of the scan group that the agent belongs to.

    Click **Next**.

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

Installing agents silently

Procedure

1. Log on to the computer where you want to install the agent as a user with administrative rights.
2. Copy the `CI27RML.tar.gz` file to a directory in the file system of your computer (either from a DVD or a directory where you store the files downloaded from Passport Advantage). Extract the compressed file into a directory on your disk.
3. Start the command-line interface and change to the directory where you have extracted the files.
4. Type: `setup.exe /z"/sf`*`drive_letter`*`:\`*`path_to_response_file_dir`*`\response_file.txt" /L`*`lang_code`* `/s`. 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 the upgrade. 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	1043 Dutch (Netherlands)
1060 Slovenian (Slovenia)	1050 Croatian	

   Example:

   ```
   setup.exe /z"/sfc:\Temp\response_file.txt" /L1033 /s
   ```

   Note: To install the agent in a custom directory, specify the directory name as the value of the environment variable:
   `ILMT_INSTALL_PATH=`*`agent_install_directory`*

Results

You have installed version 7.5 agent in silent mode.

Rerunning a failed agent installation

Agent installation consists of three phases: preinstallation, installation (copying of files) and postinstallation during which agent configuration takes place. Installation might fail during the first or third phase. The way to reinstall an agent depends on the phase during which the error occurred.

Rerunning agent installation that failed in the preinstallation phase

If the agent installation failed in the preinstallation phase, you can rerun the native installer after you have diagnosed and remedied the error.

Procedure

1. Find the cause of the problem by examining the file:

- UNIX *tivoli_common_directory*/logs/install/trace/ILMT-TAD4D-agent-pre-*date_of_the_event-hourminute*.trc
- Windows *tivoli_common_directory*\logs\install\trace\ILMT-TAD4D-agent-pre-*date_of_the_event-hourminute*.trc

2. Correct the problem. The reason of failure might be, for example, lack of sufficient write rights.
3. Retype the agent installation command.

Rerunning agent installation that failed in the postinstallation phase

If the agent installation failed in the postinstallation phase, you have two possibilities to finalize it: you can rerun the configuration process or force the installation.

Procedure

1. Find the cause of the problem by examining the file
   - UNIX *tivoli_common_directory*/logs/install/trace/traceDeployagent.log
   - Windows *tivoli_common_directory*\logs\install\trace\traceDeployagent.log
2. Correct the problem.
3. Finalize the installation.
   - Force the installation of the agent by issuing the following command:
     - AIX `installp -acFXd ILMT-TAD4D-agent-7.5-aix-ppc ILMT-TAD4D-agent`
     - HP-UX `swinstall -s reinstall=true` *ABSOLUTE_PATH_TO_INSTALLER_FILE*`/ILMT-TAD4D-agent-7.5-hpux ILMT-TAD4D-agent:<INSTALL_PATH>`
     - IBM i `RSTLICPGM LICPGM(1IBMTLM) DEV(*SAVF) RLS(V7R5M0) SAVF(`*LIBRARY_WHERE_THE_SAVF_FILE_IS_PLACED/NAME_OF_THE_SAVF*`)`
     - Linux `rpm -Uvh --force ILMT-TAD4D-agent-7.5-linux-`*platform*`.rpm`
     - Solaris `pkgadd -d ILMT-TAD4D-agent-7.5-solaris-`*platform* `ILMT-TAD4D-agent`

       Open the `/var/sadm/install/admin/default` configuration file, and change `instance=line` to `instance=overwrite` or `instance=ask`. Otherwise, the package will not be installed.
     - Windows Run the interactive installer, specifying all necessary parameters.

Installing agents on UNIX with shell installers

You can install your agents on UNIX platforms with shell installers. It is not necessary to edit and copy the response file to the target directory. All the parameters that you supply are validated on the run.

About this task

The License Metric Tool agent shell installation packages are available on the Passport Advantage website (and on the product DVD).

There are two types of shell installers:

Separate installer files for individual UNIX platforms.

- AIX `ILMT-TAD4D-agent-7.5-aix-ppc.bin`
- HP-UX `ILMT-TAD4D-agent-7.5-hpux.bin`
- Linux `ILMT-TAD4D-agent-7.5-linux-x86.bin`
- Linux `ILMT-TAD4D-agent-7.5-linux-s390.bin`
- Linux `ILMT-TAD4D-agent-7.5-linux-ppc.bin`
- Solaris `ILMT-TAD4D-agent-7.5-solaris-sparc32.bin`
- Solaris `ILMT-TAD4D-agent-7.5-solaris-sparc64.bin`
- Solaris `ILMT-TAD4D-agent-7.5-solaris-x86_64.bin`

You can get these files by extracting the file `ILMT-TAD4D-agent-7.5-shell-all.tar.gz`. Use a separate-platform shell installer if you want to install numerous agents with the same parameters on one platform.

One installer that can be used on all UNIX platforms

Run `ILMT-TAD4D-agent-7.5-multi_unix.bin` if you want to install many agents with the same parameters on different UNIX platforms. The installer recognizes the platform it is started on.

If you are installing agents on a Solaris platform that is partitioned using Oracle VM Server for SPARC technology (formerly LDOM - Logical Domains), the agent will stay in 'Incomplete' status until the agent from Global Zone on Control Domain is plugged into the server. In Logical Domains environment, agents are not able to entirely determine the underlying virtualization hierarchy. Only the agent in Global Zone on Control Domain knows about the physical computer and all other Guest Domains.

Procedure

1. Copy the compressed agent installation package `CI27RML.tar.gz` to a directory in the file system of your computer. Copy the package either from a DVD or from a directory where you store the files downloaded from Passport Advantage. Extract the compressed file into a directory on your disk. The package contains agent installers for all supported platforms.
2. Open the command-line interface and change to the directory where you store the shell installer.
3. Optional: Run the following command to obtain all the installation parameters:
   - `./`*`installer_file_name`*`.bin -get` to obtain platform-specific parameters (both types of installer: multi-UNIX and separate-platform ones),
   - `./`*`installer_file_name`*`.bin -get_all` to obtain parameters for all supported platforms (`ILMT-TAD4D-agent-7.5-multi_unix.bin` only).

   Tip: You might also want to use other options:

   -help Returns the information about available installation options.

   -extract
   Extracts the native installer and its response file to an agent temporary directory (not operating system temporary one).
4. Run the following command to set the installation parameters:
   - `./`*`installer_file_name`*`.bin -set` to set platform-specific parameters using both types of installer: multi-UNIX and separate-platform ones

- `./installer_file_name.bin -set_all` to set parameters for all platforms that you want to install the agents using `ILMT-TAD4D-agent-7.5-multi_unix.bin` only.

AIX When you install the agent on AIX, specify whether you want to install the agent in a shared WPAR. To do that:

a. Provide the default parameters. .

b. Set **InstallOnWpars** to **y** to install the agent on all shared WPARs.

If you set the option to **n**, the agent is installed on the current LPAR/WPAR.

You can install the agent in a directory different from the default one on AIX version 5.3.061 and higher by using the relocation mechanism that is based on the *User Specified Installation Location* (USIL). To install the agent in a custom location:

a. Create the *custom_location* directory:

```
mkdir -p /custom_location
```

b. Run the installation script: `./ILMT-TAD4D-agent-7.5-aix-ppc.bin -set`

c. Set the **AixCustomLocation** parameter to point to your custom location.

Solaris When you install the agent on Solaris, specify whether you want to install the agent in a local zone. To do that:

a. Run the script: `./ILMT-TAD4D-agent-7.5-solaris-sparc64.bin -set`

b. Provide the default parameters. .

c. Set **InstallOnZones** to **y** to install the agent on all zones.

If you set the option to **n**, the agent is installed in the current zone only.

Enter the following command to write default parameters to the shell installer:

`./installer_file_name.bin -restore_defaults`

5. Run the following command to install the agents: `./installer_file_name.bin -install`

   Note: Ensure that the agent certificate file is readable for any user and is located in a directory path that has read permissions set for all users. Typically, a user "nobody" or "install" is used for preinstallation checks. If a certificate file is owned by superuser and not available for reading to an installation user, the installation fails. Set the read permissions to be able to install the agent with the maximum security level.

6. Optional: If you did not use a response file, agents are configured to connect to a server on the local host. If your server is installed on a different computer:

   a. Issue the `stopsrc -s tlmagent` command to stop the agent.

   b. Edit the server location parameter in the `tlmagent.ini` file:

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

   The `tlmagent.ini` file is located in the `/etc` directory.

   c. Start the agent using the `/usr/bin/startsrc -s tlmagent` command.

7. Verify that the installation was successful, check if the agent appears as active in the web interface. If the agent does not appear after several minutes, check the installation trace logs for information about possible errors.

Results

You installed the agent on a UNIX platform.

What to do next

If you installed an agent on a logical partition (LPAR) on an AIX 5.2 host that is partitioned with workload partitions (WPARs), you must perform additional configuration steps to make sure that the server capacity is reported correctly. For more information, see Configuring the node core capacity.

Using IBM Tivoli Configuration Manager to install the agents in bulk

For environments where IBM Tivoli 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 (TMR) installed in your environment:

Table 41. Required version of Tivoli Configuration Manager and Tivoli Management Framework

Platform	Software version
IBM Power Systems	• 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
IBM System z 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.

About this task

The License Metric Tool Software Package DVD contains an agent installation SPB for each supported platform:

- AIX `agent_aix_ppc.spb`
- HP-UX `agent_hpux.spb`
- IBM i `agent_os400.spb`
- Linux `agent_linux_x86.spb`
- Linux `agent_linux_s390.spb`
- Linux `agent_linux_ppc.spb`
- Solaris `agent_solaris_32.spb`
- Solaris `agent_solaris_64.spb`
- Solaris `agent_solaris_x86.spb`
- Windows `agent_win32.spb`

Note: If you installed an agent on the computer where the stand-alone scan was run before, the list of agents show two records referring to the same computer. To fix this situation, you must manually remove the agent that belongs to the stand-alone scan group. For more information, see Removing agents.

Procedure

1. Copy the software package block (SPB) 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. When installing agents on Linux on System z provide the values for the following parameters: **MachineType**, **ProcessorType**, **SharedPoolCapacity**, **SystemActiveProcessors**, and **MessageHandlerAddress**.

   Note: When installing agents in a non-default directory, the value of the **agt_custom_location** parameter must be set to the *User Specified Installation Location* directory, for example, `agt_custom_location=/usil`.

What to do next

If you installed an agent on a logical partition (LPAR) on an AIX 5.2 host that is partitioned using workload partitions (WPARs), you must perform additional configuration steps to make sure that the server capacity is reported correctly. For more information about how to do that, see step 8 in "Installing agents on AIX using native installers".

Software package parameters

The tables list the parameters for deploying IBM License Metric Tool agents using Tivoli Configuration Manager.

Common parameters

Table 42. Common parameters

Parameter name	Description
AgentCertFilePath	If you have selected to supply certificates (**InstallServerCertificate=y**) and you are using security level 2, you need to specify the path to the 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*.
AgentTempPath	To override the location where agent keeps the working files, enter a valid path.
CITInstallPath	Specify the Common Inventory Technology installation folder.
FipsEnabled AIX UNIX	Set to *y* to enable encryption of data using a FIPS-approved algorithm. The default is *n*.

Table 42. Common parameters (continued)

Parameter name	Description
InstallServerCertificate	If you have selected **SecurityLevel=1** or **SecurityLevel=2**, you can choose to install certificates. Possible values are: **y** Install the server certificate defined in **ServerCertFilePath** or agent certificate defined in **PrivateServerCertFilePath**, or both. If **ServerCertFilePath=none**, the server test certificate will be installed. **n** Do not install any certificate file.
MessageHandlerAddress	Specify the hostname or IP address of the License Metric Tool server. Message handler is a server component which manages incoming and outgoing agent data. This is a mandatory parameter.
ProxyAddress	If **UseProxy** is *y*, enter the address (host name or IP address) of the proxy server.
ProxyPort	The port number on which the proxy server listens, if applicable. If **UseProxy** is *y*, enter the port of the proxy server.
ScanGroup	The name of a scan group that has been created in the License Metric Tool server database.
SecureAll	The port number used by the agent to communicate with the License Metric Tool server. This value is used if the level of security has been set to 2. The default is 9977.
SecureAuth	The port number used by the agent to communicate with the License Metric Tool server. This value is used if the level of security has been set to 1. The default is 9999.
SecurityLevel	The level of security to be used for communication between the agent and the License Metric Tool server. Valid values are: **0** To use nonsecure communication. **1** To use secure communications with server authentication. **2** To use secure communications with client and server authentication. **Note:** 1. The License Metric Tool 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.
ServerCertFilePath	If you have selected to supply certificates (**InstallServerCertificate=y**), 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). Use the Data Moving Service in Tivoli Configuration Manager to simultaneously copy the cert.arm file to multiple computers.

Table 42. Common parameters (continued)

Parameter name	Description
ServerCustomSSLCertificate	If you have selected to supply SSL certificate (**InstallServerCertificate=y**), you can choose to provide your own server certificate to be used by the agent for secure communications with the server. Possible values are: **y** Indicates that you want to provide your own server certificate. **n** Indicates that you want to use the server test certificate. Note that 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). If you select the value "y", you must also supply the certificate pathname (**ServerCertFilePath**). For example, to indicate that you want to use your own server certificate for SSL communication, use the following: **ServerCustomSSLCertificate=y**
ServerPort	The port number used by the agent to communicate with the License Metric Tool server. This value is used if the level of security has been set to 0. The default is 9988.
UseProxy	Set to *y* if a proxy port is to be used for communications between agents and the License Metric Tool server. The default is *n*.

Parameters for Linux on System z only

Table 43. Parameters for Linux on System z

Parameter name	Description
MachineType	Type of the machine (CP or IFL). The default is *IFL*.
ProcessorType	Type of the processor (CP or IFL). The default is *IFL*.
SharedPoolCapacity	The number of shared processors of a given type (CP or IFL) on the server
SystemActiveProcessors	The total number of processors in the computer

Solaris parameter

Table 44. Solaris parameter

Parameter name	Description
InstallOnDD	Installation on Dynamic Domain Possible 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.

Installation-related parameters (UNIX and Windows platforms)

Table 45. Installation-related parameters on UNIX and Windows platforms

Parameter name	Description
agt_logs_dir	The directory where the installer logs are to be written. The default is not to log the installation information.

Table 45. Installation-related parameters on UNIX and Windows platforms (continued)

Parameter name	Description
agt_custom_location	AIX The name of the directory in which agents are to be installed. The default value is `agt_custom_location=/usil`. Create a User Specified Installation Location (USIL) with the mkusil command if you want to install the agents in a non-standard location. This parameter is optional.
agt_temp_dir	Software Package Blocks use this folder to store temporary files.
agt_temp_path	The location of temporary agent files on the agent computer. The default value depends on the platform (`itlm` subdirectory in the temporary directory). For more information, see the related reference section.
tcm_logs_dir	The directory where the Tivoli Configuration Manager logs are to be written. The default is $(**agt_temp_path**).

Installing agents with Windows logon scripts

As an alternative to using the interactive installation wizard, you can install the IBM License Metric Tool agents on Windows targets by using the operating system facility that runs a script when users log on to the Windows domain.

About this task

The script checks if there is an agent on the computer the user has logged on, and if it detects an agent, whether it is the same version. If the script finds no agent or a back-level agent, it installs the agent.

Note: When you decided to install an agent on the computer where the stand-alone scan had been run before, the list of agents will show two records referring to the same computer. To fix this situation, you have to manually remove the agent that belongs to the stand-alone scan group. For more information, see "Removing agents".

Procedure

1. Log on 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`

You can locate those files in the .zip archive containing the latest version of the License Metric Tool agent for the Windows platform, for example, `ILMT-TAD4D-agent-7.5-windows-x86.zip`

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
   set INSTALL_PATH=INSTALL_PATH
   ```

   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 blank.

   INSTALL_PATH
   (Optional) The name of the non-default directory where you want to install the agent. If you want to use the default installation path, do not provide a value for the *INSTALL_PATH* variable. If the specified installation path contains spaces, it must be enclosed in quotes.
5. Set the agent installation parameters in the `profiles\default.conf` configuration file. You must configure parameter values for the 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 "Windows agent installation response file and logon script configuration file" on page 137
6. Log on 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

If you perform a refresh installation of IBM License Metric Tool agents, you can 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.

Procedure

1. Copy the compressed installer to a directory in the file system of your computer (either from a DVD or a directory where you store the files downloaded from Passport Advantage).
2. Open the system command line 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, there should be the following files:

   - AIX
     - `ILMT-TAD4D-agent-7.5.0.10-aix-ppc`
     - `response_file.txt`
   - HP-UX
     - `ILMT-TAD4D-agent-7.5.0.10-hpux`
     - `response_file.txt`
   - Linux
     - `ILMT-TAD4D-agent-7.5.0.10-linux-x86.rpm` or
     - `ILMT-TAD4D-agent-7.5.0.10-linux-s390.rpm` (Linux on System z, 31 and 64–bit) or
     - `ILMT-TAD4D-agent-7.5.0.10-linux-ppc.rpm` (Linux on Power Systems)
     - `response_file.txt`
   - Solaris
     - `ILMT-TAD4D-agent-7.5.0.10-solaris-x86_64` (Solaris on EM64T and AMD 64) or
     - `ILMT-TAD4D-agent-7.5.0.10-solaris-sparc32` (Solaris on SPARC, 32–bit) or
     - `ILMT-TAD4D-agent-7.5.0.10-solaris-sparc64` (Solaris on SPARC, 64–bit) and
     - `response_file.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 -s INSTALLER_FILE_NAME ILMT-TAD4D-agent
  ```

- Linux

  ```
  rpm -Uvh INSTALLER_FILE_NAME.rpm
  ```

  If the agent was installed using a native installer the command is:

  ```
  rpm -Uvh --force INSTALLER_FILE_NAME.rpm
  ```

- Solaris

  ```
  pkgadd -d INSTALLER_FILE_NAME
  ```

  If the agent was installed using a native installer, use the same command.

Results

The agent files on your computer have been refreshed.

Image cloning with preinstalled agents

Use the VM cloning feature to create a golden image with an agent that was already installed.

About this task

You can run the **tlmagent -clone** command to configure the agent to work properly after it is cloned. Then, you can clone the image and new agents will plug in to the server.

To configure the agents to work after VM images are cloned, complete the following steps:

Procedure

1. Install the agent.
2. Provide the License Metric Tool server address in the `tlmagent.ini` file.
3. Run the following command: `tlmagent -clone`
4. Clone the golden image.
5. Log on to the system that was cloned and start the agent.

   Note: If you install the agent on the golden image and plug it into the server before you run the **tlmagent -clone** command, this agent is registered on the server and displayed in the Agent window. You can remove this agent from the server.

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 IBM License Metric Tool agent on multiple Windows targets, or you can use a Windows logon script to install the agent
- "UNIX agents installation response file" on page 139

  This table shows the installation parameters that you can edit in the UNIX agent installation response files.
- "IBM i agent installation response file" on page 142

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

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 IBM License Metric Tool 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 46. Windows agent installation parameters

Parameter	**Argument**	**Default**
	Description	
Agent certificate path name	**`AgentCertFilePath`**	
	Provide the path name and file name of the agent certificate in order to add a new agent to the server with enabled MAX security level. The name of the certificate must be `key.kdb`. If the path contains spaces, enclose the whole path in double-quotes.	
Agent temporary path	**`AgentTempPath`**	*YourTempDir*\itlm
	To override the location where the agent keeps the working files, enter a valid path.	
Common Inventory Technology destination path	**`CITInstallPath`**	C:\Program Files\Tivoli\cit
	Specify the Common Inventory Technology installation folder. **Important:** Note that the Common Inventory Technology installation folder cannot be the same as or located inside the agent installation folder. **Note:** If there is already an instance of Common Inventory Technology installed on the system, this parameter will be ignored and the agent will use the existing installation of Common Inventory Technology. If the existing version of Common Inventory Technology is older, it will be upgraded during the agent installation.	
Enable Federal Information Processing Standard algorithms	**`FipsEnabled`**	n
	Specifies whether the agent is to use FIPS-approved modules in the communication of encrypted data. Possible values are *y* (yes) and *n* (no).	

Table 46. Windows agent installation parameters (continued)

Parameter	Argument	Default
	Description	
Install certificate	**InstallServerCertificate**	n
	If you have selected **SecurityLevel=1** or **SecurityLevel=2**, you can choose to install the server certificate. The possible values are *y* (yes) and *n* (no). See the **ServerCustomSSLCertificate** and **ServerCertFilePath** description below.	
Message handler address	**MessageHandlerAddress**	localhost
	Specify the hostname or IP address of the License Metric Tool server. Message handler is a server component which manages incoming and outgoing agent data.	
Port number	**Port**	9988
	Specify the port number used by the agent. This value is used for nonsecure communications (SecurityLevel=0).	
Proxy address	**ProxyAddress**	
	If **UseProxy** is set to *y*, enter the address (host name or IP address) of the proxy server.	
Proxy port	**ProxyPort**	3128
	If **UseProxy** is set to *y*, enter the port of the proxy server.	
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).	
Client authentication 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).	
Secure port number	**SecureAuth**	9999
	Specify the port number used by the agent. This value is used for secure communications with server authentication (SecurityLevel=1).	
Security level	**SecurityLevel**	0
	Determines the level of security to be used for communication between the agent and the License Metric Tool server. Possible values are: **0** To use nonsecure communication. **1** To use secure communications with server authentication. **2** To use secure communications with client and server authentication. **Note:** 1. The License Metric Tool server configured for maximum security can communicate with agents set to maximum security only. If the server is configured to use medium security, only agents set to medium or maximum security can connect to it. The 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 License Metric Tool infocenter.	
Server certificate path name	**ServerCertFilePath**	
	If you have selected to supply a server certificate (**ServerCustomSSLCertificate=y**), you must provide the path name and file name 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.	

Table 46. Windows agent installation parameters (continued)

Parameter	Argument	Default
	Description	
Server custom certificate	**ServerCustomSSLCertificate**	n
	If you have selected to supply the server certificate (**installServerCertificate=y**), you can choose to provide your own server certificate to be used by the agent for secure communications with the server. The permitted values are: **y** Indicates that you want to provide your own server certificate. **n** 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 (**ServerCertFilePath**).	
Setup type	**SetupType**	Typical
	Select **Typical** to install the agent using default values for most of the parameters except **MessageHandlerAddress** which you must specify. Select **Custom** if you want to customize other parameters.	
Use proxy	**UseProxy**	n
	Specifies whether the License Metric Tool server is protected by a proxy server. The following values are permitted: **y** The License Metric Tool server is protected by a proxy server. **n** The License Metric Tool server is not protected by a proxy server.	

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 47. UNIX agents installation parameters

Parameter	Argument	Default
	Description	
Agent certificate path name	**AgentCertFilePath**	
	Provide the path name and file name of the agent certificate in order to add a new agent to the server with enabled MAX security level. The name of the certificate must be `key.kdb`. If the path contains spaces, enclose the whole path in double-quotes.	
Agent temporary path	**AgentTempPath**	/tmp/itlm
	To override the location where agent keeps the working files, enter a valid path.	

Table 47. UNIX agents installation parameters (continued)

Parameter	Argument	Default
	Description	
Common Inventory Technology destination path	**CITInstallPath**	
	Specify the Common Inventory Technology installation folder. **Important:** Note that the Common Inventory Technology installation folder cannot be the same as or located inside the agent installation folder. **Note:** If there is already an instance of Common Inventory Technology installed on the system, this parameter will be ignored and the agent will use the existing installation of Common Inventory Technology. If the existing version of Common Inventory Technology is older, it will be upgraded during the agent installation.	
Disable rollback	**disableRollBack=y**	
	Add this parameter to the response file to disable the automatic rollback of changes to the system in case of a failed installation. This preserves the failed installation on your computer, and allow you to examine it to discover the reasons for the failure.	
Enable Federal Information Processing Standard algorithms	**FipsEnabled**	n
	Specifies whether the agent is to use FIPS-approved modules in the communication of the encrypted data. The possible values are *y* (yes) and *n* (no).	
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. The 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	
Install server certificate	**InstallServerCertificate**	n
	If you have selected **SecurityLevel=1** or **SecurityLevel=2**, you can choose to install the server certificate. Possible values are *y* (yes) and *n* (no). See the **ServerCustomSSLCertificate** and **ServerCertFilePath** descriptions below.	
Linux on System z: Machine type	**MachineType**	z9
	Specify the type of physical machine Linux 390 is running on. The possible values are: **z9** If you are installing the agent on any machine older than z10 e.g. system z9, z990, or S/390®. **z10** If you are installing the agent on a z10 or z196 server computer.	
Message handler address	**MessageHandlerAddress**	localhost
	Specify the hostname or IP address of the License Metric Tool server. Message handler is a server component which manages incoming and outgoing agent data.	
Port number	**Port**	9988
	Specify the port number used by the agent. This value is used for nonsecure communications (SecurityLevel=0).	
Linux on System z: Processor type	**ProcessorType**	IFL
	Specify the type of processors the Linux image is running on. The possible values are: **CP** Your Linux image is running on CP processors. **IFL** Your Linux image is running on IFL processors. This parameter is required for the installation to succeed.	
Proxy address	**ProxyAddress**	
	If **UseProxy** is *y*, enter the address (host name or IP address) of the proxy server.	

Table 47. UNIX agents installation parameters (continued)

Parameter	Argument	Default
	Description	
Proxy port	**ProxyPort**	
	If **UseProxy** is *y*, enter the port of the proxy server.	
Scan group name	**ScanGroup**	DEFAULT
	The name of the scan group to which the agent belongs. The agent can be reassigned to another scan group by the License Metric Tool server, or by the inventory administrator on the server. The name of the scan group cannot contain any special characters (e.g. spaces).	
Client authentication 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).	
Secure Port	**SecureAuth**	9999
	Specify the port number used by the agent. This value is used for secure communications with server authentication (SecurityLevel=1).	
Security level	**SecurityLevel**	0
	Determines the level of security to be used for communication between the agent and the License Metric Tool 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 License Metric Tool 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 License Metric Tool infocenter.	
Server certificate path name	**ServerCertFilePath**	
	If you have selected to supply a server certificate (**ServerCustomSSLCertificate=y**), you must provide the path name and file name of the certificate. The name of the certificate must be `cert.arm`. If the path contains spaces, enclose the whole path in double-quotes.	
Server custom certificate	**ServerCustomSSLCertificate**	n
	If you have selected to supply the server certificate (**InstallServerCertificate=y**), you can choose to provide your own server certificate to be used by the agent for secure communications with the server. The permitted values are: **y** Indicates that you want to provide your own server certificate. **n** 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 *y*, you must also supply the certificate path name (**ServerCertFilePath**).	

Table 47. UNIX agents installation parameters (continued)

Parameter	Argument	Default
	Description	
Linux on System z: Shared pool capacity	**SharedPoolCapacity**	
	If the Linux on System z 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 on System z: Node capacity	**SystemActiveProcessors**	
	If the Linux on System z 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.	
Use Proxy	**UseProxy**	n
	Specifies whether the License Metric Tool server is protected by a proxy server. The following values are permitted: **y** The License Metric Tool server is protected by a proxy server. **n** The License Metric Tool server is not protected by a proxy server.	

IBM i agent installation response file

This table shows the installation parameters that you can edit in the IBM i 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 48. IBM i agents installation parameters

Parameter	Argument	Default
	Description	
Install certificate	**InstallServerCertificate**	n
	If you have selected **SecurityLevel=1** or **SecurityLevel=2**, you can choose to install certificates. Possible values are: **y** Install the server certificate defined in **ServerCertFilePath** or agent certificate defined in **PrivateServerCertFilePath**, or both. If **ServerCertFilePath=none**, the server test certificate will be installed. **n** Do not install any certificate file.	
Message handler address	**MessageHandlerAddress**	
	Specify the hostname or IP address of the License Metric Tool server. Message handler is a server component which manages incoming and outgoing agent data. This is a mandatory parameter.	
Port number	**Port**	9988
	Specify the port number used by the agent. This value is used for nonsecure communications (**SecurityLevel=0**).	

Table 48. IBM i agents installation parameters (continued)

Parameter	Argument	Default
	Description	
Proxy address	**ProxyAddress**	
	If **UseProxy** is *y*, enter the address (host name or IP address) of the proxy server.	
Proxy port	**ProxyPort**	
	If **UseProxy** is *y*, enter the port of the proxy server.	
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 License Metric Tool server, or by the inventory administrator on the server.	
Client authentication 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**).	
Secure port	**SecureAuth**	9999
	Specify the port number used by the agent. This value is used for secure communications with server authentication (**SecurityLevel=1**).	
Security level	**SecurityLevel**	0
	Determines the level of security to be used for communication between the agent and the License Metric Tool server. Possible values are: **0** To use nonsecure communication. **1** To use secure communications with server authentication. **2** To use secure communications with client and server authentication. **Note:** 1. The License Metric Tool 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 License Metric Tool infocenter.	
Server certificate path name	**ServerCertFilePath**	
	If you have selected to supply certificates (**installServerCertificate=y**), 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).	

Table 48. IBM i agents installation parameters (continued)

Parameter	**Argument**	**Default**
	Description	
Use Proxy	**UseProxy**	n
	Specifies whether the License Metric Tool server is protected by a proxy server. The following values are permitted: **y** The License Metric Tool server is protected by a proxy server. **n** The License Metric Tool server is not protected by a proxy server.	

Chapter 4. Uninstalling

This section provides instructions for uninstalling the IBM License Metric Tool servers, database and agents.

Uninstalling the License Metric Tool servers and databases

The uninstallation 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.

If only License Metric Tool is installed within Tivoli Integrated Portal, the uninstaller will remove both products.

You must uninstall the product before you can install it again on the same computer. 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 backup of the database before uninstalling. Then, restore the backup to populate the database that you have installed on the new computer. See Moving the TLMA database to a separate server 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

Use the uninstallation wizard to specify the parameters for the uninstallation (either with embedded, or base WebSphere Application Server).

Before you begin

The interactive uninstallation mode requires graphical user interface (GUI) on your computer. For UNIX platforms, ensure that your computer has a graphical user interface such as X Window System.

About this task

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

Procedure

1. Depending on whether your operating system belongs to the Windows family or UNIX-class family, start the uninstallation wizard in the following way:

   UNIX

   a. Start uninstaller.sh.

   Windows

   a. Select the **Add/Remove Programs** option from the Control Panel.

b. Select **IBM License Metric Tool**.
c. Click **Remove**.

2. On the welcome screen, click **Next** to start uninstallation.
3. The wizard detects the elements that are present on the computer. Clear any that you do not want to uninstall. Leave the option to drop the TLMA database selected if appropriate.

   If an error is generated when attempting to drop the database, you can manually drop the database with the DB2 command `db2 drop database tlma`. *tlma* is the name of the License Metric Tool database.
4. Click **Next**. The wizard displays a panel showing the Tivoli Integrated Portal credentials. Provide the user name and password and click **Next**.
5. The wizard displays a panel showing the elements to be uninstalled and other actions to be completed. Click **Uninstall** to continue with the uninstallation. The panel that opens shows the summary of uninstallation actions and their statuses.
6. When the uninstallation is complete, the uninstaller lists all the completed actions. Click **Done** to exit from the wizard.

Results

You have uninstalled the License Metric Tool server and database.

What to do next

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

If you installed the administration server on an existing instance of Tivoli Integrated Portal, this instance is not removed.

In order to delete the License Metric Tool logs, you must delete the contents of the Tivoli Common Directory (if no other IBM Tivoli application uses that directory to store its logs).

Uninstalling the server in silent mode

When the uninstall program runs in silent mode, it uses the parameters provided in a response file.

About this task

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

The uninstallation program is located in the directory *INSTALL_DIR*`\Uninstall`.

Use the command-line interface to run the uninstaller in silent mode.

Procedure

1. Log on the computer where you want to run the uninstaller with Administrator or root rights.

2. Change to the *INSTALL_DIR*\Uninstall 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, run the uninstall script (uninstall.bat for Windows and uninstall.sh for other platforms) with the following parameters:
   - Linux UNIX uninstall.sh -f *absolute_path_to_response_file* -i silent
   - Windows uninstall.bat -f *absolute_path_to_response_file* -i silent

   Example:

   Windows
```
uninstall.bat -f "C:\Program Files\IBM\LMT\Uninstall\
uninstallresponse.txt" -i silent
```

Results

The IBM License Metric Tool uninstallation process runs in silent mode.

What to do next

You can now delete the License Metric Tool logs from Tivoli Common Directory (if no other IBM Tivoli application uses that folder to store its logs).

Tip: The uninstaller does not remove WebSphere Application Server or DB2. It does not delete any user groups created during the DB2 installation, either.

The server and database uninstallation response file

The uninstallresponse.txt file, which is provided with IBM License Metric Tool, is an InstallAnywhere options file. It defines arguments to set each parameter required by the License Metric Tool uninstallation wizard.

Table 49. Server and database silent uninstallation parameters

Parameter	Parameter key name	Default
	Description	
Uninstalling the administration server element	**RSP_UNINSTALL_ADMIN**	false
	Specifies whether the License Metric Tool element is to be uninstalled. The possible values are: **true** The server is to be uninstalled. **false** The server is not to be uninstalled. This parameter is ignored if the server is not installed on the computer.	
Uninstalling the License Metric Tool database element	**RSP_UNINSTALL_ADMDB**	false
	Specifies whether the License Metric Tool administration server database component is to be uninstalled. Possible values are: **true** The database is to be uninstalled. **false** The database is not to be uninstalled. This parameter is ignored if the element is not installed on the computer. **Note:** You can uninstall the administration server database component without dropping the TLMA database and deleting the tlmsrv user.	

Table 49. Server and database silent uninstallation parameters (continued)

Parameter	Parameter key name	Default
	Description	
Uninstalling databases: drop database	**RSP_UNINSTALL_TLMA**	true
	Specifies whether the TLMA database on this computer is to be deleted. The possible values are: **true** The database is to be dropped. **false** The database is not to be dropped.	
Removing the tlmsrv user	**RSP_UNINSTALL_TLMSRV**	true
	Specify if the tlmsrv user account created on a target computer is to be deleted. The possible values are: **true** The tlmsrv user is to be removed. **false** The tlmsrv user is not to be removed.	
Tivoli Integrated Portal administrator user ID	**RSP_TIP_ADMIN_NAME**	tipadmin
	Tivoli Integrated Portal administrator's name	
Tivoli Integrated Portal administrator password	**RSP_TIP_ADMIN_PASSWD**	
	Tivoli Integrated Portal administrator's password	
Shutting down all running processes to uninstall the administration server	**RSP_AUTO_CLOSE_PROCESSES**	false
	Specifies if the silent installer shuts down the running processes. To enable this option, uncomment the following line: `RSP_AUTO_CLOSE_PROCESSES=true` **Note:** 1. You do not need to specify this option to stop the server as it stops automatically. 2. Only the processes that are recognized are shut down automatically.	

Uninstalling 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.

Before you begin

Important: Do not put any files into agent installation directory - this directory should only contain agent files and data. Agent installation directory will be removed during uninstallation.

Uninstalling License Metric Tool 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.

Procedure

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`.

What to do next

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.

About this task

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 License Metric Tool agents using the tlmunins script" on page 148.

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.

About this task

If you installed an agent on WPAR in a relocated directory, or if you installed an agent on WPAR with shared global (read-only) `/usr` and `/opt` directories, do not use the `tlmunins.sh` script. You must run the **installp** command to uninstall the agent.

Procedure

1. Open a system command prompt.
2. Enter the following command:
   - **installp -u ILMT-TAD4D-agent**
   - In WPAR environments, use the following command:

     ```
     installp -u -Or ILMT-TAD4D-agent
     ```
   - If you want to uninstall the agent installed in a custom location (*USIL*), add the additional parameter **-R**:

     ```
     installp -R /path_to_usil -u ILMT-TAD4D-agent
     ```

What to do next

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

Uninstalling HP-UX agents

Uninstall HP-UX agents using the **swremove** command.

Procedure

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

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

What to do next

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

Uninstalling IBM i agents

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

Before you begin

Stop the agent before uninstallation.

Procedure

1. Open the system command line.
2. Enter the following command:

   ```
   DLTLICPGM LICPGM(1IBMTLM)
   ```

What to do next

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

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.

Procedure

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

   ```
   rpm -e ILMT-TAD4D-agent-7.5
   ```

What to do next

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

Uninstalling Solaris agents

Uninstall Solaris agents using the **pkgrm** command.

About this task

You can uninstall the agent in a global zone. If there are any agents installed in local zones set in this global zone, you need to uninstall them separately.

If you uninstall the agent from Global Zone on Control Domain in Logical Domains (LDOM) environment, bear in mind that all other agents on Control Domain and any other Guest Domains will turn to 'Incomplete' status on server. This is because of the fact that only this particular agent is able to report the entire virtualization hierarchy.

Procedure

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

   ```
   pkgrm ILMT-TAD4D-agent
   ```

What to do next

To complete the uninstallation, you must remove the agent in the administration console. See *Removing agents in the administration console*.

Uninstalling Windows agents

Uninstall Windows agents using the uninstallation wizard.

Procedure

1. Start the uninstall wizard.
   a. Select the **Add/Remove Programs** option from the Control Panel.
   b. Select **ILMT-TAD4D Agent version 7.5**.
   c. Click **Remove**.
2. Click **OK** to commence the uninstallation.
3. When the uninstallation is completed, click **Finish** to exit from the wizard.

   Note: If you cancel the uninstallation, the agent is stopped. To restart the agent use the **tlmagent** command.

Results

You have uninstalled the agent on a Windows computer.

What to do next

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

Removing agents

You can remove agents form the table. For example, these could be agents that are *not connecting* to the server.

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.

Procedure

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**.

Results

Removing agents that are *not connecting*

When you remove agents that are not connecting to the server, 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. You can still see the agent information in old audit reports, for example.

If agents have not communicated with the server for the time period specified in the maxAgentInactivityToDelete parameter, they are automatically unregistered from the server.

Removing active agents

If you accidentally or intentionally remove an active agent, it automatically registers back the next time it contacts the server, and appears in the table as well.

Appendix.

Review the following additional information before you install IBM License Metric Tool.

Starting the server

To start the server, you must run the `srvstart.bat` or `srvstart.sh` script. If the server does not start after running the script, you must start the DB2 instance and rerun the script.

Procedure

1. Go to the directory <*INSTALL_DIR*>/cli, where <*INSTALL_DIR*> is the name of the License Metric Tool installation directory.
2. Run the following script:
   - Windows `srvstart.bat`
   - UNIX `srvstart.sh`
3. Optional: If your server does not start after running the script, you must start your DB2 instance. By default, DB2 instances that were created during the installation on the Windows operating system are set to autostart. To set up DB2 to autostart, do the following steps:
   a. Log on to the computer where DB2 is installed with the DB2 administrator ID and password that were specified at the installation time.
   b. UNIX On UNIX computers, run the following script: `$INSTHOME/sqllib/db2profile`
   c. Type `db2start` at the command line. The DB2 instance starts.
   d. Stop the server and start it by repeating steps 1 and 2.

Stopping the server

When you are stopping the server, you might also consider stopping the DB2 database software.

Procedure

1. Go to the directory <*INSTALL_DIR*>/cli, where <*INSTALL_DIR*> is the name of the License Metric Tool installation directory.
2. Run the `srvstop.bat` (Windows) or `srvstop.sh` (UNIX) script.

   Tip: On Linux and UNIX, you are prompted for the user administrator ID and password. Optionally, you can use the parameters **`-username`** and **`-password`** when you run the `srvstop.sh` script.
   The server stops.
3. Additionally, you may want to stop the DB2 instance.
   a. Log in to the machine where DB2 is installed with the DB2 administrator ID and password specified at installation time.
   b. Type `db2stop` at a DB2 command line.

   The DB2 instance stops.

Server installation problems

Find out more about common problems that might occur during server installation, or uninstallation.

About this task

- "Server installation problems on AIX operating system"

  Sometimes problems may occur during installation. Recognize the symptoms of the problem and find the solution.
- "Server installation problems on Solaris operating system" on page 155

  Find the description that matches the problem you encounter and follow the instructions to solve it.
- "Server installation problems on UNIX operating systems" on page 156

  Identify the problem with server installation that you are dealing with and the instructions how to solve it.
- "Server installation problems on Windows operating system" on page 157

  Find the solution to the problem you encountered when installing on a Windows platform.
- "Database problems" on page 161

  During server installation, problems with database may occur. Find the description of the problem and follow the instructions to solve it.
- "Other installation problems" on page 162

  If during the installation, you encountered a problem that is not platform-specific and does not suit any category of problems described in the **Server installation and uninstallation problems** section, look for the solution here.

Server installation problems on AIX operating system

Sometimes problems may occur during installation. Recognize the symptoms of the problem and find the solution.

The list below contains common installation problems that may occur on AIX platforms:

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.

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.

While installing License Metric Tool on AIX 6.1 with DB2 9.1, a DB2 installation error occurs.

The *Tivoli_common_dir*/COD/logs/install/trace/DB2install.log file contains information on minor DB2 installation error: `ERROR:mkdev: 0514-519 The following device was not found in the customized device configuration database: name = 'aio0'`

ERROR:An error occurred while enabling Asynchronous I/O. DB2 requires Asynchronous I/O to be enabled to function properly. Enable this manually using "smit aio". If the problem persists contact a technical service representative. Select the step *Installing DB2* as successful and continue the installation.

Server installation problems on Solaris operating system

Find the description that matches the problem you encounter and follow the instructions to solve it.

The list below contains descriptions of common problems that may occur when installing on the Solaris operating system:

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 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.

When installing on Solaris or HP-UX operating systems, creating and populating the server database fails and the following error occurs: `CODIN0035E An error occurred while populating the 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.

Server installation fails on Solaris 10 SPARC platform during the creating and populating of the database. The following message is recorded in the `trace_db_servers.log` file: `SQL3306N An SQL error "-1218" occurred while inserting a row into the table. SQL1218N There are no pages currently available in bufferpool "4096"`.

The problem may be caused by DB2 V9.1 or 9.5 self-tuning memory mechanism. It can be resolved by the installation of the latest DB2 fix pack. If the problem persists, disable Self-Tuning Memory Manager and configure DB2 manually. For more information refer to: http://publib.boulder.ibm.com/infocenter/db2luw/v9r5/index.jsp?topic=/com.ibm.db2.luw.admin.config.doc/doc/r0006017.html .

Server installation problems on UNIX operating systems

Identify the problem with server installation that you are dealing with and the instructions how to solve it.

The list below contains descriptions of common installation problems on UNIX:

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 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.

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.

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 License Metric Tool: installation documentation for more information about resuming a failed installation. To solve the problem, start the DB2 services and resume the installation.

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 fails on SUSE Linux Enterprise Server 11 Service Pack 2 and the following message is displayed: `Incorrect platform. This image is for Linux x86 64bit, check the documentation if your platform is supported!`

To solve the problem, open the script `ILMT-server-7.5-linux-x86_64.sh'/ 'TAD4D-server-7.5-linux-x86_64.sh` and remove the following section:

```
if [ -s "$SCRIPT_DIR/../tools/getArch" ]
then
 . "$SCRIPT_DIR/../tools/getArch"
 if [ "$PLATFORM_EXPECTED" != "$ILMTA" ]
 then
  if [ -n "$ILMTA_DESC" ]
  then
   print -u2 "Incorrect platform. This image is for $PLATFORM_EXPECTED_DESC,
   You should use image for $ILMTA_DESC instead!"
  else
   print -u2 "Incorrect platform. This image is for $PLATFORM_EXPECTED_DESC,
   check the documentation if your platform is supported!"
  fi
  exit 1
 else
  print "Running installation wizard for $PLATFORM_EXPECTED_DESC"
 fi
else
 print -u2 "Unable to load helper script $SCRIPT_DIR/../tools/getArch"
fi
```

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.

License Metric Tool Launchpad cannot be started on UNIX platforms.

When starting the License Metric Tool Launchpad from the hard disk of your UNIX computer, ensure that the path to the launchpad executable file (`launchpad.sh`) does not contain spaces.

Uninstaller does not remove product installation directory on HP-UX.

If you find some files and directories in `/opt/IBM/LMT/jre` after the uninstallation of the administration server on HP-UX, remove them manually.

When installing on Solaris or HP-UX operating systems, creating and populating the server database fails and the following error occurs: `CODIN0035E An error occurred while populating the 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.

Server installation problems on Windows operating system

Find the solution to the problem you encountered when installing on a Windows platform.

The list below contains descriptions of common problems that may occur on Windows operating system:

The installation wizard running in unattended mode on a Windows platform does not recognize the presence of the DB2 server.

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.

The Launchpad does not start on a Windows computer

The following message is displayed:

```
The ordinal 325 could not be located in the dynamic link library SHDOCVW.dll.
```

The reason for this error might be that Internet Explorer is not fully initialized (registered). The problem appears only on computers with newly installed Windows operating system. To remedy the situation restart the server and then start the Launchpad again by running `launchpad.exe`.

The installation of Tivoli Integrated Portal fix pack on Windows ends with error 16.

The installation has failed because it was started from a location with a path name longer than 40 characters. To solve the problem, start the installation in a directory with a very short name, located on the top level of the directory tree of the computer hard drive disk, for example `C:\fp`.

Tivoli Integrated Portal fix pack installer files cannot be extracted from compressed file with standard Windows tools

When you extract the contents of the compressed file using built-in zip archive support, you are asked for a password. The reason for this error is that the zip file containing the fix pack has files with very long file paths. To remedy this problem, use a dedicated application such as 7-Zip.

Tivoli Integrated Portal-related installation problems

Identify the problem with Tivoli Integrated Portal that you are dealing with and read the instructions how to solve it.

The list below contains the descriptions of common installation problems with Tivoli Integrated Portal:

The installation of IBM License Metric Tool failed in such way, that Tivoli Integrated Portal is unable to continue working or the uninstallation of License Metric Tool has left Tivoli Integrated Portal uninstalled.

To manually uninstall Tivoli Integrated Portal:

1. Check if there are no applications running on Tivoli Integrated Portal - enter the following command:

   WAS_home_dir`/profiles/TIPProfile/bin/tipRegister -isEmpty`

   It must return **`true`**.
2. Force the removal of Tivoli Integrated Portal - enter the following command:

   WAS_home_dir`/profiles/TIPProfile/bin/zaptip`

The installation of Tivoli Integrated Portal fix pack on Windows ends with error 16.

The installation has failed because it was started from a location with a path name longer than 40 characters. To solve the problem, start the installation in a directory with a very short name, located on the top level of the directory tree of the computer hard drive disk, for example `C:\fp`.

The installation of Tivoli Integrated Portal has failed with return code 255 (message CODBB0022E).

The reason for the failure is unknown. Try to remedy the installation by performing the following steps:

1. Ensure that you have enough available RAM that is required by the product.
2. Ensure that you have enough disk space.
3. Ensure that you are installing the server on a supported operating system.

If these actions do not help, contact IBM software support.

The installation of Tivoli Integrated Portal fix pack 2.2.0.3 has failed and it is not possible to install the fix pack without removing some files manually.

The complete removal and reinstallation of License Metric Tool is not possible due to the remaining `acsi` folder. To solve the problem, contact IBM software support.

Troubleshooting installation of Tivoli Integrated Portal fix pack 2.2.0.7

You might encounter impediments, limitations, and problems while you install Tivoli Integrated Portal fix pack 2.2.0.7. To facilitate the installation process, refer to the requirements and tips.

Logs

The main installation log that is created by the installer of the Tivoli Integrated Portal fix pack is in your root directory:

- Windows *%USERPROFILE%*`\TIPFPInstaller-*.log`
- UNIX `$HOME/TIPFPInstaller-*.log`

Additional logs for the individual fix pack installation steps are in the installation directory of Tivoli Integrated Portal or base WebSphere Application Server:

- *TIP_INSTALLATION_DIR*`/logs`
- *BASE_WAS_INSTALLATION_DIR*`/logs`

Especially important are the files: `validatePrereqs.err` and `validatePrereqs.out`.

Space requirements

The installation of the fix pack requires:

- More than 1 GB of free disk space, mainly in the existing installation directory of Tivoli Integrated Portal and the temporary directory of your operating system
- About 1 GB of free RAM, where at least 128 MB should be available while the fix pack installer is already running. To avoid potential problems, provide 2 GB of free RAM.

More information about fix pack prerequisites can be found in the following file: *TIP_FP_INSTALLATION_IMAGE_DIR*/COI/PackageSteps/TIPInstall_PreCheck-FP7/FILES/TIPInstall_PreCheck-FP7.cfg

File path limitations

When you fill in the response files, pay special attention to the *IAGLOBAL_TIP_HOME* variable:

- Ensure that the file path does not end with / \ or \\
- Windows Use \\ as a separator
- Windows Use an uppercase letter to denote a disk drive
- Windows You must enter the Tivoli Integrated Portal directory in the same case that you used during the installation of the GA version of the application.

FIT tool

The Tivoli Integrated Portal installer requires an additional tool: the FIT suite. You can download the package from the IBM FixCentral website.

Before Tivoli Integrated Portal fix pack is applied, the FIT files must be extracted to the following directory of the target instance, :

- Windows `C:\Program Files\IBM\TIP9\profiles\TIPProfile\etc\fit`
- UNIX `/opt/IBM/TIP9/profiles/TIPProfile/etc/fit`

The FIT directory contains the following files:

- `fit.bat`
- `fit.sh`
- `FIT.jar`

Failed installation

If the installation fails, open the `TIPFPInstaller-*.log` fix pack installation log and find the following line that is at the bottom of the log:

`SEVERE : Aborting installer: $variable_defining_error`

The most common problems for failed installation and their causes are listed below:

- `IAGLOBAL_INVALID_TIP_LOCATION`: the installer could not locate the existing installation of the Tivoli Integrated Portal or the found installation is not a correct one.
  - The problem can be caused by a difference between bitness of the installer and the existing Tivoli Integrated Portal installation.
  - Windows Check the Tivoli Integrated Portal installation path that is defined in your response file. Use an uppercase letter to denote a disk drive.
  - Windows Use \\ as the path separators and do not leave separator at the end of your path.
- `IAGLOBAL_INVALID_USERID_OR_PASSWORD`: wrong user or password was provided. Use the credentials for the Tivoli Integrated Portal administrator. The default user name is `tipadmin`
- `IAGLOBAL_INVALID_PREREQS`: the amount of disk space or free memory is insufficient. Check the log files: `validatePrereqs.out` and `validatePrereqs.err`

The installation of Tivoli Integrated Portal fix pack 2.2.0.7 failed and it is not possible to install the fix pack without removing some files manually. The complete removal and reinstallation of License Metric Tool is not possible due to the remaining `acsi` folder that might be common for other applications. To solve the problem, contact IBM software support.

Database problems

During server installation, problems with database may occur. Find the description of the problem and follow the instructions to solve it.

The list below contains descriptions of common database problems that may occur during installation:

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

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`.

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*`/lmt7.5.0/Server.log` 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.

When installing the 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.

The installation, uninstallation, or upgrade of License Metric Tool database fails and the cause of the failure is not known.

There might be different reasons for this, for example incorrect DB2 password or one that has just expired. Check the su.log file for possible reasons of the failure. Examples:

```
- Tue Dec 15 17:20:19 CET 2009 - Executing: su - db2inst4 -c
"cd /opt/IBM/LMT/admin/db/db2 && ./dbinstall.sh true"
 su: incorrect password
```

```
-  Tue Dec 15 17:49:55 CET 2009 - Executing: su - db2inst4 -c
"cd /opt/IBM/LMT/admin/db/db2 && ./dbuninstall.sh"
Password change requested. Choose a new password.
Old Password:
```

For more information see Server installation and upgrade trace logs.

Other installation problems

If during the installation, you encountered a problem that is not platform-specific and does not suit any category of problems described in the **Server installation and uninstallation problems** section, look for the solution here.

The following list contains descriptions of common installation problems:

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.

The installation does not start - console mode detected.
The situation occurs when the installation or uninstallation process stops right after its execution, and there is the Console mode detected entry in the ia.log, or in the ServerUninstall.log file. You can also find in the trace_servers.log, and in the msg_servers.log files the following error message: CODIN0414E Console mode is not supported.

It means that you have tried to start the installation or uninstallation process interactively, however, you machine does not support any window system. Try to install such system, set the display appropriately or simply run the installation in the silent mode. For more information, see: Installing the server in silent mode or Uninstalling in silent mode.

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 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 License Metric Tool 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 License Metric Tool server requires at least 770 MB free memory to deploy and 1 GB to run.

The installation has been broken and cannot be resumed.
Uninstall the server and install it again.

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 1 GB free to deploy and 3 GB to run with the database installed.

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 run time 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 installation 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.

The server installation wizard displays the information that the `master.tag` file cannot be found and installation cannot continue even though the files have been removed from the file system.
The problem occurs because the appropriate entries have not been removed from the InstallAnywhere product registry. First, back the `.com.zerog.registry.xml` file up, and then manually remove all entries referring to License Metric Tool. The exact location of this directory depends on the operating system:

- `/var/.com.zerog.registry.xml` (UNIX-based systems)
- `\Program Files\Zero G Registry\.com.zerog.registry.xml` (Windows)

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 server has not correctly plugged in to WebSphere Application Server. To resolve the problem, you must regenerate the Web server plug-in configurations. To do this, complete the following steps:

1. Start the WebSphere Administrators 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 server.

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, License Metric Tool works only on WebSphere Application Server internal transports. ReinstallWebSphere Application Server shortening the path, then reinstall License Metric Tool.

Unable to uninstall the product whose installation process was broken during the installation phase.

When similar error message shows up during uninstallation to this one: `java.lang.IllegalArgumentException: No product for ID=dc44d3c4-1ef2-11b2-afa7-b6ef25df9157`, you must delete the product files manually and start the installation process again.

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.

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 Data Source 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 `<Tivoli_common_dir>/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 the programs that use a lot of memory before you start the installation.

The `cleanupWAS` script fails while undeploying the administration server.

During the uninstallation, the **`cleanupWAS`** script fails while undeploying the License Metric Tool administration server. In order to identify the problem, check the logs for the `FileNotFoundException` information. In order to successfully undeploy the server, restart WebSphere Application Server and run the script again.

The connection to the database fails during the installation process, even though user has provided the correct password for the tlmsrv login or the password is not accepted by the server installer.

The connection to the License Metric Tool server database fails during the installation process, even though user has provided the correct password for the **tlmsrv** login (DB2 is to be reused). The user might also be asked to provide the password twice (which happens when the database is installed for the first time). The problem seems to be the binary file for the pluggable authentication module, which probably is not working properly or it cannot start. To prevent the problem from occurring turn on the NO-PAM mode by setting the parameter `RSP_ENABLE_NO_PAM_MODE` to `=true` in the server installation response file.

The installation has failed with the message CODIN0496E. The verification of IBM Deployment Engine has failed.

During the installation an instance of Deployment Engine was found and modified. As a result of the modification, it became corrupted, and cannot be used now. To resolve the problem, contact IBM software support.

The installation failed with the message CODIN0378E. An internal exception has occurred while reading a host name.

The error indicates that there is a problem with resolving the server hostname. Check the network configuration of the server: the hostname and IP address. You can use the **`nslookup`** command to view domain name and IP address details. For example:

1. Enter the following command to retrieve the hostname:
   ```
   hostname
   ```
2. Enter the following command to verify the resolved IP address:
   ```
   nslookup current_hostname
   ```

Check the details returned by **`nslookup`**. The hostname must be correctly resolved. If the hostname is incorrectly resolved, refer the problem to your system administrator.

Troubleshooting agent installation and uninstallation

Find out more about common problems that might occur during agent installation, or uninstallation.

About this task

Agent installation problems on AIX platforms

When installing the agent on an AIX machine, you may encounter one of the common installation problems. Find the description that matches your problem and solve it

The list below contains common agent installation problems on AIX:

On AIX, the native installer hangs after installation. The agent is installed successfully, but the status is not changed to success. The following message is displayed: `Some entries in the next screen do not have the correct string length. Check your language environment variable and the code set.`

This error occurs when the packages `bos.loc.com.utf` and `bos.loc.utf.EN_US` are installed on the system, and the **LANG** environmental variable is set to **EN_US**.

Change the value of the **LANG** variable in `/etc/environment` from **EN_US** to **en_US**, or type `LANG=en_US` to change the value for the current session only.

On AIX, after upgrading the server from version 7.1 to 7.2.x, 7.5 or 7.5 fix pack 1, the agent version 7.1 stops sending scheduled software scans.

To solve this problem, stop the agent, delete its cache and start the agent.

When installing an agent, the following message is displayed: "CODAG099E Installing of the Common Inventory Technology (CIT) infrastructure element SPB has failed. Installation cit failed".

To find out more, run the following command: *INSTALL_PATH*`/utilities/cit/wcitinst i 5724-D33 -s` *INSTALL_PATH*`/utilities/cit/cit.spb -d` *CIT_INSTALL_PATH*

where the default Common Inventory Technology installation path is `/opt/tivoli/cit`

Installation of an agent in a User Specified Installation Location (USIL) fails and the following message is displayed: `ERROR: Check disk space for directory "/opt/tivoli/cit/" error.install: Failed while executing the ILMT-TAD4D-agent.pre_i script.`

There are two reasons for this error: the WPAR has the directory in `/opt` in read-only mode, and the relocated installation forces Common Inventory Technology (CIT) installer to try to install CIT in `/opt/tivoli/cit`.

Solution: If you install agent on AIX, on an LPAR using customized CIT location (provided in `response_file.txt`) and you are about to install the agent on a WPAR (hosted by the LPAR mentioned above) CIT installation path needs to be customized to point to the directory with read/write rights accessible from the WPAR.

Installation of an agent on AIX LPAR fails.

When you are installing an agent on AIX LPAR, the following message is returned by the command-line interface:

```
installp -acgXd ILMT-TAD4D-agent-7.5-aix-ppc ILMT-TAD4D-agent
Could not load program /usr/sbin/restbyname:
System error: Not enough space
installp: The specified device <location>/ILMT-TAD4D-agent-7.5-aix-ppc is not a valid device
```

The problem might occur because the *XPG_SUS_ENV* variable is set to ON and prevents the execution of the program due to memory constraints on the static data. To solve the problem, you must change the settings of the *XPG_SUS_ENV* variable.

- To change the settings temporarily for a particular user session, run the **unset XPG_SUS_ENV** command.
- To change the settings permanently, go to the user profile and change the value of the *XPG_SUS_ENV* variable to OFF.

Uninstallation is successful, but GSKit directory is still in use by an LPAR process, and cannot be removed.

After removing an agent from a workload partition (WPAR), the GSKit directory on the WPAR still exists, which means that a file cannot be removed from the WPAR directory. To remove the file, restart the WPAR.

Uninstallation of an agent from a WPAR on AIX fails.

Uninstallation did not complete because the use of the `tlmunins.sh` script is not supported on WPAR in a relocated directory, or on WPAR with shared global (read-only) `/usr` and `/opt` directories on AIX.

To uninstall the agent, enter the following command:

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

Agent installation problems on Linux operating system

Solve the problems that you may encounter during agent installation on Linux platforms.

Find the description that matches your problem and follow the instructions to solve it:

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 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`.

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**.

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`

Although the installation on an agent fails, the system reports a successful installation.

When the problem occurs, complete the following steps:

1. Execute the following uninstallation command: **`rpm -e`** *ILMT-TAD4D-agent*
2. If the uninstallation fails, use the command: **`rpm -e --noscripts`** *ILMT-TAD4D-agent*
3. If the target directory for the agent has been created, delete it.
4. If there are is an `/etc/tlmagent.ini` file left, delete it.

When installing an agent, the following message displays: "CODAG099E Installing of the Common Inventory Technology (CIT) infrastructure element SPB has failed. Installation cit failed".

To find out more, run the following command: *`INSTALL_PATH`*`/utilities/cit/wcitinst i 5724-D33 -s` *`INSTALL_PATH`*`/utilities/cit/cit.spb -d` *`CIT_INSTALL_PATH`*

where the default Common Inventory Technology installation path is `/opt/tivoli/cit`

Installation of agent fails on Security-Enhanced Linux and the following message displays: "/var/itlm/gskit/bin/gsk7ver: error while loading shared libraries: /var/itlm/gskit/lib/libgsk7krsw.so: cannot restore segment prot after reloc: Permission denied".

GSKit binary files cannot run in SE Linux, for example `/var/itlm/gskit/bin/gsk7ver`, if text relocation is turned on. To turn off the checking of text relocation in GSKit packages run the following commands after changing to the agent directory:

```
setsebool -P allow_execmod=1
./tlmagent -g
```

Agent installation problems on IBM i, Windows and Solaris platforms

Solve the problems that may occur during agent installation.

Follow the instructions to solve the problem that you have encountered:

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.

When installing an agent on Solaris using native installers, the following message is displayed: `WARNING: The <depends> package "SUNWcsu Core Solaris, (Usr)" is a prerequisite package and should be installed.`

It does not mean that the prerequisite is not installed, but that an element required during the agent installation is being checked.

During agent installation on Windows or Solaris, the following message is displayed: "CODAG099E Installing of the Common Inventory Technology (CIT) infrastructure element SPB has failed. Installation cit failed".

To find out more, run the following command:

- on Solaris, *INSTALL_PATH*`/utilities/cit/wcitinst i 5724-D33 -s` *INSTALL_PATH*`/utilities/cit/cit.spb -d` *CIT_INSTALL_PATH*

  where the default Common Inventory Technology installation path is: `/opt/tivoli/cit`
- on Windows, *INSTALL_PATH*`\utilities\cit\wcitinst.exe i 5724-D33 -s` *INSTALL_PATH*`\utilities\cit\cit.spb -d` *CIT_INSTALL_PATH*

  where the default Common Inventory Technology installation path is:
  - on Windows `C:\Program Files\Tivoli\cit`
  - on Windows 64-bit `C:\Program Files(x86)\Tivoli\cit`

After you uninstalled the Windows agent, the `itlm_msi_cache` directory is left either in the `%WIN_DIR%` or in the temporary directory.

You can safely delete the `itlm_msi_cache` directory.

During agent installation on IBM i, the following error is displayed: `chown: 001-0070 Exception MCH3402 not expected`

To solve the problem, check the setting of the environment variable *QIBM_MALLOC_TYPE*. If the variable is set to `DEBUG` on the `*JOB` or `*SYS` level, delete the setting.

Other agent installation problems

Find the solution to problems that you encountered during agent installation.

Choose the description that matches the problem that occurred when you were installing the server and follow the instructions to solve it.

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.

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 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/`

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 cannot be uninstalled by system native installation tools after it has been upgraded from version 2.3 or 7.1 to 7.2.x, 7.5 or 7.5 fix pack 1 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.

Agent native installation fails, either during the preinstallation or postinstallation phase.
The process of installing agents natively consists of three phases:

1. Preinstallation
2. Installation (copying of files)
3. Postinstallation (configuration)

If the installation fails during the first phase, you might get the following error message:
```
Preparing...
########################################## [100%] error:
%pre(ILMT-TAD4D-agent-7.5.0.10.i386) scriptlet failed, exit status
exit_code
```

If the installation fails during the third phase, you might get the following error message:
```
Preparing...
########################################## [100%] error:
%post(ILMT-TAD4D-agent-7.5.0.10.i386) scriptlet failed, exit status
exit_code
```

You need to rerun the agent installer. For information how to do it see Rerunning a failed agent installation.

Installing of agents in bulk using customer-specific tools fails.
One of the possible reasons why this happens is because the customer-specific tools that deploy agents on a large number of computers set the value in the **current_working_directory** parameter to **null** (when running a new process on an endpoint). To prevent agent installation failures set the value to **non-null** (when possible).

Agent native installation fails because of missing Global Security Toolkit prerequisite.

To check what prerequisites are missing, run the following script: *agent_install_path*/gskit/private_checkinstall. You should get listing similar to the one below:

```
Required Patch 108435-14 missing
Required Patch 111327-05 found
Required Patch 108991 found
Required Patch 108993-31 found
Required Patch 108528-29 found
Required Patch 113648-03 found
Required Patch 116602-01 found
Required Patch 111317-05 found
Required Patch 111023-03 found
Required Patch 115827-01 found
```

Search your operating system vendor's Web site and download the patch (in the example above 108435-14). Install the patch and rerun the agent native installation.

Agent installation fails because of incorrect Common Inventory Technology installation directory.

Common Inventory Technology cannot be installed in the agent installation directory. If the value of the **CITInstallPath** parameter in the agent installation response file specifies an installation directory the same as or located inside the agent installation directory, the agent installation fails.

If your agent installation or upgrade fails due to this problem, uninstall the old agent and install the newer version from scratch.

The agent installation completes, but the following message is displayed during installation: `A logger of class ccg_pdlogger could not get the host name. The host name will not be logged. The system reports the command has been successfully executed.`

The DNS hostname could not be resolved. The hostname of a machine that has an agent installed on it must resolve in the DNS to the machine's IP address. You should configure hostname resolution for your machine correctly, per the DNS configuration rules for your operating system.

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.
1623-14, Shimotsuruma, Yamato-shi
Kanagawa 242-8502 Japan

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law:
INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those 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.

Trademarks

IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at “Copyright and trademark information” at www.ibm.com/legal/copytrade.shtml.

Intel, Intel logo, Intel Inside, Intel Inside logo, Intel Centrino, Intel Centrino logo, Celeron, Intel Xeon, Intel SpeedStep, 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 or registered trademarks of Oracle and/or its affiliates.

Index

L

N

O

P

R

S

T

U

V

W

Printed in USA

GC14-7637-02