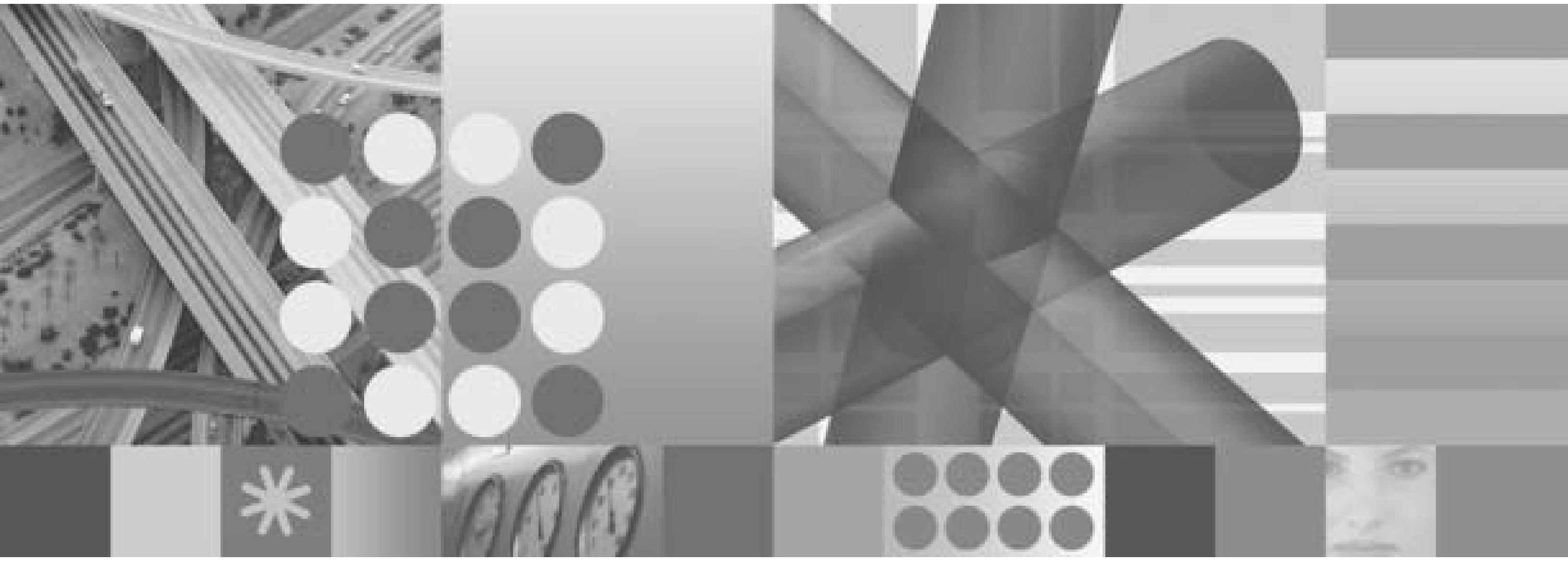
Tivoli® Configuration Manager

Version 4.3.1



License Management with License Compliance Manager Version 2.3 fix pack 4

SC23-6140-01

Note

Before using this information and the product it supports, read the information in Appendix C, “Notices,” on page 125.

This edition applies to version 4 release 3 modification level 1 of IBM Tivoli Configuration Manager (program number 5724-C06) and to all subsequent releases and modifications until otherwise indicated in new editions.

Contents

Preface

The purpose of this guide is to describe how you can implement IBM Tivoli License Compliance Manager license management facilities in your IBM Tivoli Configuration Manager version 4.3.1 environment.

This guide explains how to plan, install, and configure the environment, as well as license management use scenarios that demonstrate the license management extension facilities.

Who should read this guide

This guide is intended for administrators who want to implement license management facilities in their IBM Tivoli Configuration Manager, version 4.3.1 environment.

Readers should be familiar with the following topics:

- Windows operating systems
- Tivoli environment
- IBM Tivoli Configuration Manager environment
- Supported database architectures and concepts

Publications

This section lists publications in the IBM Tivoli Configuration Manager library and related documents. It also describes how to access Tivoli publications online and how to order Tivoli publications.

IBM Tivoli Configuration Manager library

The following documents are available in the IBM Tivoli Configuration Manager library:

- *Release Notes*, GI11-0926

  Contains the latest information about this release of IBM Tivoli Configuration Manager, including installation and upgrade notes; software limitations, problems, and workarounds; documentation notes; and internationalization notes.
- *Introducing IBM Tivoli Configuration Manager*, GC23-4703

  Explains the concepts of IBM Tivoli Configuration Manager and its components and provides a road map to the IBM Tivoli Configuration Manager documentation.
- *User's Guide for Software Distribution*, SC23-4711

  Explains the concepts and procedures necessary to effectively distribute software over networks using the Software Distribution component of IBM Tivoli Configuration Manager.
- *Reference Manual for Software Distribution*, SC23-4712

  Provides in-depth information about the IBM Tivoli Configuration Manager commands used by the Software Distribution component and explains advanced features, concepts, and procedures necessary to effectively use the Software Distribution component.

- *User's Guide for Inventory*, SC23-4713

  Explains the concepts and procedures necessary to effectively use the Inventory component of IBM Tivoli Configuration Manager and provides in-depth information about the commands used by the Inventory component.
- *Messages and Codes*, SC23-4706

  Provides details of the messages generated by the IBM Tivoli Configuration Manager components.
- *Inventory Online Help*

  Provides related information about using the Inventory graphical user interface (GUI).
- *Database Schema Reference*, SC23-4783

  Describes the IBM Tivoli Configuration Manager database tables.
- *User's Guide for Deployment Services*, SC23-4710

  Describes the common support and management tasks provided by Deployment Services for Software Distribution and Inventory.
- *IBM Tivoli Configuration Manager: Patch Management Guide*, SC23-5263

  Describes how you can implement an automated patch management solution in a Windows environment, taking advantage of the functions provided by IBM Tivoli Configuration Manager version 4.3.1.
- *IBM Tivoli Configuration Manager: Guide for Microsoft Active Directory Integration*, SC32-2285

  Describes how you can integrate the Microsoft Active Directory environment with the Tivoli environment.
- *IBM Tivoli Configuration Manager: User's Guide for Operating System Deployment Solution*, SC32-2578

  Describes how you can implement an operating system imaging solution.

Related publications

The following documents also provide useful information:

- *Tivoli Management Framework: Planning for Deployment Guide*, GC32-0803

  Explains how to plan for deploying your Tivoli environment. It also describes Tivoli Management Framework and its services.
- *Tivoli Management Framework: Reference Manual*, GC32-0806

  Provides in-depth information about Tivoli Management Framework commands. This manual is helpful when writing scripts that are later run as Tivoli tasks. This manual also documents default and validation policy scripts used by Tivoli Management Framework.
- *Tivoli Management Framework User's Guide*, GC32-0805.

  Describes the concepts and procedures for using Tivoli Management Framework services.

The *Tivoli Software Glossary* includes definitions for many of the technical terms related to Tivoli software. The *Tivoli Software Glossary* is available at the following Tivoli software library Web site:

http://publib.boulder.ibm.com/tividd/td/link/tdprodlist.html.

Access the glossary by clicking the **Glossary** link on the left pane of the Tivoli software library window.

Accessing terminology online

The *Tivoli Software Glossary* includes definitions for many of the technical terms related to Tivoli software. The *Tivoli Software Glossary* is available at the following Tivoli software library Web site:

http://publib.boulder.ibm.com/tividd/glossary/tivoliglossarymst.htm

The IBM Terminology Web site consolidates the terminology from IBM product libraries in one convenient location. You can access the Terminology Web site at the following Web address:

http://www.ibm.com/software/globalization/terminology

Accessing publications online

The product CD contains the publications that are in the product library. The format of the publications is PDF, HTML, or both. To access the publications using a Web browser, open the `infocenter.html` file. The file is in the appropriate publications directory on the product CD.

IBM posts publications for this and all other Tivoli products, as they become available and whenever they are updated, to the Tivoli software information center Web site. Access the Tivoli software information center by first going to the Tivoli software library at the following Web address:

http://publib.boulder.ibm.com/tividd/td/link/tdprodlist.html

Scroll down and click the **Tivoli Product manuals** link. In the Tivoli Technical Product Documents Alphabetical Listing window, click the <**IBM Tivoli Configuration Manager**> link to access the product library at the Tivoli software information center.

Note: If you print PDF documents on other than letter-sized paper, set the option in the **File →Print** window that allows Adobe Reader to print letter-sized pages on your local paper.

Ordering publications

You can order many Tivoli publications online at the following Web site:

http://www.elink.ibmlink.ibm.com/public/applications/ publications/cgibin/pbi.cgi

You can also order by telephone by calling one of these numbers:

- In the United States: 800-879-2755
- In Canada: 800-426-4968

In other countries, contact your software account representative to order Tivoli publications.

Tivoli technical training

For Tivoli technical training information, refer to the following IBM Tivoli Education Web site:

http://www.ibm.com/software/tivoli/education

Support information

If you have a problem with your IBM software, you want to resolve it quickly. IBM provides the following ways for you to obtain the support you need:

- Searching knowledge bases: You can search across a large collection of known problems and workarounds, Technotes, and other information.
- Obtaining fixes: You can locate the latest fixes that are already available for your product.
- Contacting IBM Software Support: If you still cannot solve your problem, and you need to work with someone from IBM, you can use a variety of ways to contact IBM Software Support.

For more information about these three ways of resolving problems, see Appendix B, “Support information,” on page 119.

Conventions used in this guide

This guide uses several conventions for special terms and actions, operating system-dependent commands and paths, and margin graphics.

Typeface conventions

This guide uses the following typeface conventions:

Bold

- Lowercase commands and mixed case commands that are otherwise difficult to distinguish from surrounding text
- Interface controls (check boxes, push buttons, radio buttons, spin buttons, fields, folders, icons, list boxes, items inside list boxes, multicolumn lists, containers, menu choices, menu names, tabs, property sheets), labels (such as **Tip:**, and **Operating system considerations**:)
- Keywords and parameters in text

Italic

- Words defined in text
- Emphasis of words (words as words)
- New terms in text (except in a definition list)
- Variables and values you must provide

`Monospace`

- Examples and code examples
- File names, programming keywords, and other elements that are difficult to distinguish from surrounding text
- Message text and prompts addressed to the user
- Text that the user must type
- Values for arguments or command options

Operating system-dependent variables and paths

This guide uses the UNIX convention for specifying environment variables and for directory notation.

When using the Windows command line, replace **$***variable* with **%***variable***%** for environment variables and replace each forward slash (**/**) with a backslash (****) in directory paths. The names of environment variables are not always the same in Windows and UNIX. For example, %TEMP% in Windows is equivalent to $tmp in UNIX.

Note: If you are using the bash shell on a Windows system, you can use the UNIX conventions.

Chapter 1. Overview

The IBM Tivoli Configuration Manager license management extension provides license management facilities in your Configuration Manager environment.

It provides license management facilities using IBM Tivoli License Compliance Manager. It is not a full implementation of License Compliance Manager, but rather an extension of your existing Configuration Manager environment. The solution is released with IBM Tivoli Configuration Manager, Version 4.3.1. For further updates to this solution, refer to the IBM Tivoli Configuration Manager product support Web site: http://www-306.ibm.com/software/sysmgmt/products/support/IBMTivoliConfigurationManager.html.

This overview provides you with introductory information about License Compliance Manager and its integration into the Configuration Manager environment. It includes the following topics:

- "What is License Compliance Manager?"
- "New concepts and components"
- "Features, advantages, and benefits" on page 4
- "License Compliance Manager implications" on page 5
- "Impact on Configuration Manager" on page 6

What is License Compliance Manager?

IBM Tivoli License Compliance Manager identifies distributed software inventory and use to help manage software costs and contract compliance in a distributed environment.

This software asset management solution helps IT to align software spending with business priorities. With the information provided, organizations can reduce unnecessary software costs and compliance risks to allocate additional resources to priority projects.

The web-based GUI helps a software asset manager to quickly obtain the information needed to make decisions. License Compliance Manager consolidates information about products installed and software use. It controls how a license is to be used using predefined license types, reports on compliance situations, and unlicensed use. It supports the creation of license information using electronic entitlement file import. License Compliance Manager maintains historical software use information and provides XML-exportable reports, in both online and batch mode, that assist in forward planning for license needs by comparing figures for created, installed, and used licenses. It can also generate alerts when license use reaches a defined level. Using License Compliance Manager's flexible architecture you can scale the installation to fit your needs, while ensuring security of confidential information through security profiles for access to the Web interface, and by transmitted data encryption.

New concepts and components

The license management extension introduces some new concepts and components in the Configuration Manager topology.

The following concepts and components are introduced for the Configuration Manager license management extension implementation:

License Compliance Manager Administration server

Each License Compliance Manager installation has a single administration server. The administration server runs on WebSphere® Application Server. This server is responsible for agent plug-in, upload of potential signatures, and upload of inventory information and software use. The administration server provides the following facilities:

- A repository of product, license agreement, license use, installed software, and organization information.
- A Web interface you can use to perform license management and administration tasks and to produce historical reports of license use and inventory information over time.
- A command-line interface that you use to import electronic license entitlements, manage complex products, and massive data import, as well as system management and problem determination tasks.
- The capability to generate and send e-mails to provide notification when license use thresholds are reached or exceeded.
- The capability to reconcile license information defined on the Web Interface with the software use information received from agents.

Federated databases

License Compliance Manager and Configuration Manager maintain a set of common information in their databases. Both applications store information about installed software and about hardware configuration of the target machines. To keep this information synchronized between the two databases, the databases store duplicate information. To avoid data inconsistency, a synchronization mechanism at the endpoint uploads the same information for both applications when common information is requested. Figure 1 on page 3 represents the federated databases containing their own application-specific data, together with hardware and software inventory duplicate data. The DB2® services, apply and capture, maintain the database federation. See Chapter 8, “Maintaining the federated databases,” on page 51 for more information about the database federation.

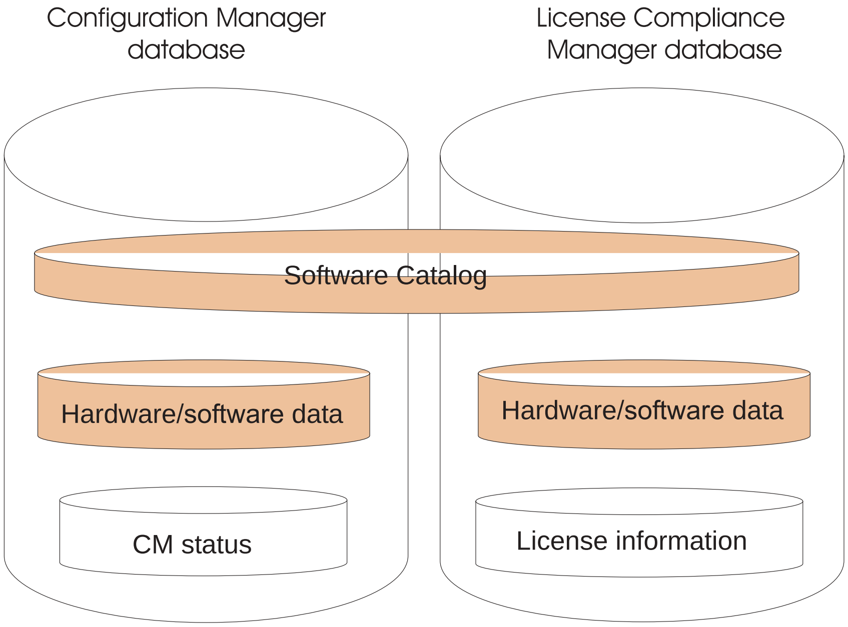


Figure 1. Federated databases

An Inventory profile that is configured to perform a scan for installed products using signature matching is distributed to an endpoint. After completing collection, a License Compliance Manager software scan is invoked to prepare the same set of information. Both groups of information are uploaded to the Tivoli® server using MCollect, the Configuration Manager Scalable Collection Service component. The License Compliance Manager and Inventory database tables that maintain the result of the software signature scan are updated with the same set of information. Accessing this information from either application interface results in the same set of information. The agent is started to collect hardware information. Inventory is invoked to prepare the same set of information and both are uploaded to the Tivoli server using MCollect.

License Compliance Manager Catalog manager

The License Compliance Manager catalog manager component maintains the master catalog of products that you want to discover and monitor. The catalog includes information about the products that can be monitored and the signatures that are used by the agent to detect the presence and use of products on monitored computers. You can also use the catalog manager to process potential signatures and link them to new or existing products. The catalog information is stored in tables in the administration server database. Each product in the catalog has a hierarchical structure made up of the product, version of the product, and releases of each version. The component has a graphical interface you use to perform various tasks.

License Compliance Manager agent

A License Compliance Manager agent must be deployed on each Tivoli endpoint that is to be monitored by License Compliance Manager. The agent performs the following functions:

- Performs an inventory of the software installed on the computer and forwards this information to the License Compliance Manager administration server.
- Identifies software products that are running to collect information about the use of monitored software products on the monitored computer. The

agent stores this information in its cache and uploads it to the administration server at regular, configurable intervals.

- Collects information about software that is running on the monitored computer that is not included in the catalog of software products and adds it to a list of potential signatures. You can then process the potential signatures and link them to new or existing products using the License Compliance Manager catalog manager tool.

Configuration Manager Extension for License Manager

The Configuration Manager Extension for License Manager component is made up of the License Compliance Manager Data Handler and the License Compliance Manager handler. The data files are uploaded from the endpoints to the gateway collector. The License Compliance Manager Data Handler retrieves agent data from the gateway collector and transfers it to the License Compliance Manager handler for upload to the administration server database. The existing Tivoli server in your Configuration Manager environment offers the agents services similar to those offered by the runtime server in the full implementation of License Compliance Manager. It assumes the role of supporting communication between the administration server and the agents.

Configuration Manager Endpoint Extension

The Configuration Manager Endpoint Extension is distributed to the endpoints by an Inventory dependency. It handles the data from the Configuration Manager endpoints and the License Compliance Manager agents and transfers the data to the gateway collector.

Features, advantages, and benefits

The Configuration Manager license management extension offers the following features.

The Tivoli License Compliance Manager licensing facilities implemented in your Configuration Manager environment provide your organization with the following:

Common extended signature catalog

Both Configuration Manager and License Compliance Manager use the Common Inventory Technology (CIT) 2.5 scanning technology. CIT 2.5 supports several new signature types that are not supported with previous versions of CIT. The software scan is modified to use complex signatures. As a result, the format of the catalog has changed and software scanners on the endpoints require the signature catalog to discover which signatures are present on the endpoint. License Compliance Manager also provides you with a signature catalog management tool. You can use this tool to expand and make changes to the list of products that can be monitored for licensing purposes.

With the federated database technology, data in the Configuration Manager configuration repository database and the License Compliance Manager administration server database is synchronized and can be easily retrieved and delivered as if all the data was local. Both products share the same catalog and maintain a set of common information such as, installed software and hardware configuration of the target machines. The databases maintain duplicate information accessible by the current interfaces provided by the two applications. To avoid data inconsistency, a synchronization mechanism is implemented at the endpoint to upload the same information for both applications when common information is requested.

Generate significant cost savings

Tivoli License Compliance Manager helps verify that businesses pay only for the software they need and use. By linking software installation and license use to product entitlements and contracts, it can assist you in knowing exactly what software licenses you have, which ones are being used, and which ones you might need.

Signature management

Catalog manager. The catalog manager is a tool that you can use to expand and make changes to the list of products that can be monitored for licensing purposes.

Increase productivity

With the information gained from License Compliance Manager, businesses can plan for future software changes and prioritize internal support and maintenance for only the most-used applications.

IBM® WebSphere integration

The WebSphere infrastructure makes it possible to deploy or upgrade License Compliance Manager across multiple applications simultaneously. It also permits complete license management using a simple Web-browser interface, regardless of location.

Thin-client architecture

Tivoli License Compliance Manager offers decentralized thin-client administration for optimal flexibility. User access privileges can be controlled by assigning users a predefined role based on their responsibilities. Users can complete license management tasks using a simple Web-browser interface, regardless of their location.

Extensive license model support

Able to manage several types of software licensing models, including CPU-based, User-based, Machine-based, Concurrent-use, Multi-use, and more. Tracks software deployment and use according to the specific licensing model subscribed to effective license management.

License Compliance Manager implications

If you implement the license management extension in your Configuration Manager environment you might not have all the License Compliance Manager functions and, in some cases, you might have functions not available with License Compliance Manager.

The license management extension is not a full implementation of License Compliance Manager but rather an extension of Configuration Manager to include license management facilities using IBM Tivoli License Compliance Manager. The license management extension has the following limitations:

- All agents must be assigned to one single organization. The license management extension does not allow you to create more than one organization.
- The License Compliance Manager method of distributing the updated catalog and agent configuration information (agent information, division information, scan frequency) is not used in the license management extension environment. Instead, the updated catalog and agent configuration information is included in a software package and is downloaded to the agents using the **wtlminfoget** command. For more information, see “wtlminfoget” on page 74. The Configuration Manager Extension for License Manager component installed on the Tivoli server permits the Administration server to communicate with the Tivoli server as if it were a runtime server.

- License Compliance Manager implements a synchronization mechanism between the main components of the architecture to ensure that the data collected on the endpoints is reliable for licensing reports. In the Tivoli Management framework environment such a synchronization mechanism cannot be maintained and a new implementation has been designed providing a lower level of licensing reports reliability, due to an inaccurate calculation of the highwater mark.
- Sub capacity licensing limitations. Configuration Manager does not support partitioning. To exploit sub capacity licensing you must either implement the full version of License Compliance Manager, or configure your environment to manage the coexistence of both environments. See “Expanding the limited implementation to the full version” on page 105 and “Coexistence between limited and full version of License Compliance Manager” on page 105.
- The license management extension does not use the License Compliance Manager runtime server. A new component is installed on the Tivoli management region server (or on a managed node) that allows the administration server to recognize the Configuration Manager Extension for License Manager as a runtime server.
- SSL is not supported because the License Compliance Manager agent communicates through the Tivoli Framework using Tivoli Framework security support. The administration server must work within the same intranet as the Tivoli management region server.

The license management extension also provides the following additional functionality that is not available with License Compliance Manager:

- The default division to which an agent is assigned at installation time can be modified, one time only, after the agent has been installed. In a License Compliance Manager environment, this capability is not available, and the division must be specified when the agent is installed.

Impact on Configuration Manager

With the implementation of the license management extension, some Configuration Manager tasks are not available or are performed differently.

The following is a list of Configuration Manager tasks that have changed with the License Compliance Manager implementation:

- The Inventory Administration graphical user interface is no longer used to import signatures. The License Compliance Manager catalog manager tool is the interface used for signature management.
- A new policy region is added to your Tivoli environment containing a profile manager and a task library with a number of predefined tasks and jobs.

Chapter 2. Planning the license management extension topology

This section provides an overview of the factors you must consider when you implement License Compliance Manager to monitor the installed software, software use, and license compliance in your Configuration Manager environment.

The following topics provide you with information to help you plan your implementation:

- "Configuration Manager license management extension topology"
- A high-level overview of the steps involved to implement the extension. See "Road map" on page 10
- "Supported platforms" on page 11
- "Prerequisites" on page 16

Configuration Manager license management extension topology

When you implement License Compliance Manager in your Configuration Manager environment, you are introducing some new components.

Table 1 lists the components required for the license management extension and the Tivoli resource on which the components reside.

Table 1. Configuration Manager license management extension components

Component	**Resource**
Description	
License Compliance Manager administration server and database	Any computer. Although the server and database can reside on the same computer, it is recommended that they be located on separate computers. The machine requirements for these elements are described in the *IBM Tivoli License Compliance Manager: Planning, Installation, and Configuration*
An additional computer is required in your Configuration Manager environment to host the administration server. The administration server should be on a dedicated computer and run on WebSphere Application Server. The administration server database is a DB2 repository of product, license agreement, license use, installed software, and organization information.	
License Compliance Manager agents	Endpoints
A license management agent must be deployed on each endpoint computer to be monitored. The agent collects information about the software installed and running on the computer. There are two methods available to install Tivoli License Compliance Manager agents on Tivoli endpoints. See Chapter 5, "Deploying and configuring agents," on page 33 for more details on these methods.	
Configuration Manager Extension for License Manager	Tivoli management region server / managed node

Table 1. Configuration Manager license management extension components (continued)

<table>
<tr><th>Component</th><th>Resource</th></tr>
<tr><th colspan="2">Description</th></tr>
<tr><td colspan="2">This component must be installed first on the Tivoli server, and then optionally, on other managed nodes, provided that the node already has the Inventory server and Software Distribution server components installed. It includes the License Compliance Manager Data Handler and the License Compliance Manager handler. The License Compliance Manager Data Handler retrieves agent data from the gateway collector and transfers it to the License Compliance Manager handler for upload to the administration server database. The Configuration Manager Extension for License Manager is initially active only on the Tivoli server, but you can transfer it to another node if the Tivoli server becomes overloaded. See “Transferring the extension component to a different location” on page 48.

In an interconnected environment, you can install this component in another region, but you must manually register the Tivoli server on the administration server before it can be used by agents. To register the server, use the **Manage Infrastructure->Servers->Create** task from the portfolio of the administration server Web interface. The Tivoli server is registered as a runtime server and the runtime serve name is the name registered in the tlm_extension.ini file at installation time. Refer to the *IBM Tivoli License Compliance Manager: Administration* for more information about registering a server.

It includes the installation of the License Compliance Manager Data Handler which is responsible for transferring agent data to the License Compliance Manager administration server. The License Compliance Manager Data Handler is installed only the first time you install the Configuration Manager Extension for License Manager component. The License Compliance Manager Data Handler can run on any managed node. To avoid performance degradation, install or move it to a different computer than the computer where the Inventory Data Handler is running if possible.

It is installed in the $BINDIR/TME/TLM_EXT directory and, by default, uses the $DBDIR/tlm_handler and $DBDIR/tlm_data_handler directories as the working directories.See “wtlmdh” on page 71 for ways you can interact with the License Compliance Manager Data Handler.</td></tr>
<tr><td>Configuration Manager Endpoint Extension</td><td>Endpoint</td></tr>
<tr><td colspan="2">This component is installed on all gateways, and at the first distribution of an inventory profile, it is installed on the endpoints connected to the gateway. It handles the data from the Configuration Manager endpoints and the License Compliance Manager agents and transfers data to the gateway collector.</td></tr>
<tr><td>Catalog manager</td><td>Managed node/Tivoli management region server</td></tr>
<tr><td colspan="2">This License Compliance Manager infrastructure element must be installed on the Tivoli server if you plan to import signatures using packages. You can optionally install this element, on those managed nodes where you plan to import signatures and manage the IBM Software catalog using the **winvsig** command. The catalog manager is the preferred method for managing signatures.</td></tr>
</table>

Figure 2 on page 9 shows the Configuration Manager license management extension components in the Configuration Manager environment.

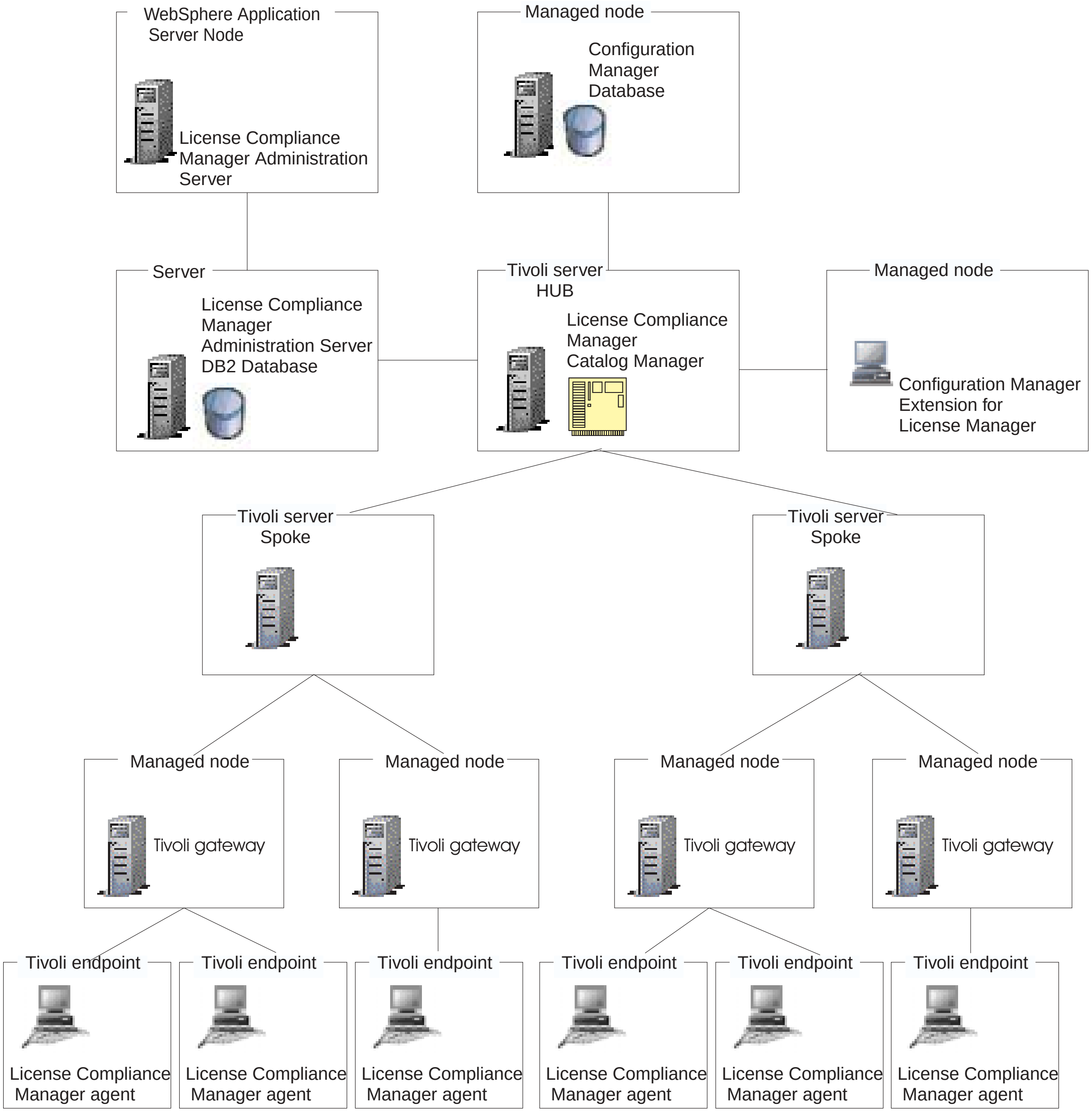

WebSphere Application Server Node
License Compliance Manager Administration Server
Managed node
Configuration Manager Database
Server
License Compliance Manager Administration Server DB2 Database
Tivoli server HUB
License Compliance Manager Catalog Manager
Managed node
Configuration Manager Extension for License Manager
Tivoli server Spoke
Tivoli server Spoke
Managed node
Tivoli gateway
Managed node
Tivoli gateway
Managed node
Tivoli gateway
Managed node
Tivoli gateway
Tivoli endpoint
License Compliance Manager agent
Tivoli endpoint
License Compliance Manager agent
Tivoli endpoint
License Compliance Manager agent
Tivoli endpoint
License Compliance Manager agent
Tivoli endpoint
License Compliance Manager agent
Tivoli endpoint
License Compliance Manager agent

Figure 2. Configuration Manager license management extension topology

Note: You can install the Configuration Manager Extension for License Manager on any of the spoke regions in this topology, but you must remember to manually register the Tivoli server on the License Compliance Manager administration server before it can be used by agents. To register the server, use the **Manage Infrastructure->Servers->Create** task from the portfolio of the administration server Web interface. The Tivoli server is registered as a runtime server and the runtime serve name is the name registered in the tlm_extension.ini file at installation time. Refer to the *IBM Tivoli License Compliance Manager: Administration* for more information about registering a server.

Road map

A road map gives a high-level view of how to implement the license management extension in your environment.

This road map assumes that the IBM Tivoli Configuration Manager has been installed in your environment. To implement the license management extension in your Configuration Manager environment and make it ready for use, you must complete the following tasks:

Table 2. Steps to get license management facilities up and running

Step	Task	For details ...
1	Plan the license management extension topology.	Chapter 2, “Planning the license management extension topology,” on page 7
2	Back up the Inventory configuration repository database.	**DB2 database** DB2 Information Center http://publib.boulder.ibm.com/infocenter/db2luw/v8//index.jsp **Oracle database** Refer to Oracle technical documentation for details.
3	Install the Configuration Manager license management extension components: Configuration Manager Endpoint Extension, Configuration Manager Extension for License Manager included in the Configuration Manager CD.	“Installing and upgrading the license management extension components” on page 19.
4	Install the following License Compliance Manager infrastructure elements: administration server, administration server database, catalog manager.	Packaging information and installation steps are described in *IBM Tivoli License Compliance Manager: Planning, Installation, and Configuration*. See “Installing the license manager extension support” on page 28 for installation instructions for the administration server database that are specific to the Configuration Manager license management extension.
5	Prepare the Inventory configuration repository and the administration server databases for the federation. **Note:** If the configuration repository is an Oracle database, this step includes the installation of the Oracle client and WebSphere Information Integrator on the computer where the License Compliance Manager administration server database is installed.	“Preparing your databases for the federation” on page 24. The WebSphere Information Integrator installation images can be downloaded from the License Compliance Manager support Web site http://www-306.ibm.com/software/sysmgmt/products/support/IBMTivoliLicenseManager.html.
6	Deploy and configure agents	Chapter 5, “Deploying and configuring agents,” on page 33
7	Manage agents	Chapter 7, “Managing agents,” on page 45

Table 2. Steps to get license management facilities up and running (continued)

Step	Task	For details ...
8	Maintaining the federated databases	Chapter 8, “Maintaining the federated databases,” on page 51

See “Troubleshooting the installation” on page 77 for topics that can help you perform problem determination during the installation process.

Supported platforms

This section provides information about the platforms on which the Configuration Manager license management extension is supported. It also provides information about these platforms.

The supported platforms are the platforms in common with both Configuration Manager and License Compliance Manager. The supported platforms are divided into the following categories:

- “Supported platforms for servers, databases, and catalog manager”
- “Agent and endpoint platforms” on page 13

Supported platforms for servers, databases, and catalog manager

Table 3 lists the platforms on which License Compliance Manager servers, databases, and the catalog manager can be installed and includes information about the minimum maintenance level required. It also applies to the supported platforms of the Tivoli management region server (Tivoli server).

Table 3. Supported platforms for servers, databases, and catalog manager

Platform		
Operating system	**Version**	**Level, service packs, patches**
Windows®	XP Professional	
	Server 2003 Standard or Enterprise Edition	
	Server 2003 Standard or Enterprise Edition (32-bit) for Intel® x86	
	Server 2003 Standard or Enterprise Edition (64-bit) on EMT64 and AMD64 (supported only for administration server and database, not Tivoli server)	
	Server 2000	
	Server 2000 Advanced	
IBM AIX	6.1 (64-bit)	
	5.3 (32-bit)	
	5.3 (64-bit)	
	5.2 (32-bit)	
	5.2 (64-bit)	

Table 3. Supported platforms for servers, databases, and catalog manager (continued)

Platform		
Operating system	**Version**	**Level, service packs, patches**
HP-UX	11i v2 on PA-RISC	Patch PHSS_35381
	11i v3 on PA-RISC	
	11i for PA-RISC 2.0 (64-bit, in 32-bit compatibility mode)	Patch PHSS_33033
	11i v1 on PA-RISC	
	11i v2 running on rx7640 and rx8640	Patch PHKL_35174 **Note:** This patch is required when agents are deployed in partitioned environments.
Red Hat Enterprise Linux®	ES/AS/WS 4.0 for EM64T and AMD64	
	ES/AS/WS 4.0 (32-bit) for x86	Update 3
	ES/AS/WS 3.0 (32-bit) for x86	
	4.0 for Power	Update 2
	AS, version 4.0 for IBM iSeries and pSeries (64-bit)	
	AS, version 3.0 for IBM iSeries and pSeries (64-bit)	Update 1
	AS, version 4.0 for IBM zSeries and IBM S/390 (64-bit) on 64-bit hardware	
	AS, version 3.0 for IBM zSeries and IBM S/390 (31-bit)	
SUSE Linux Enterprise Server	10 for Power	
	10 for IBM zSeries and IBM S/390 (64-bit) on 64-bit hardware	Service Pack 3
	10 for x86 (64-bit)	
	10 for x86 (32-bit)	
	10 for IBM iSeries/pSeries (64-bit)	
	10 for EMT64 and AMD64	
	9 for Power	
	9 for IBM zSeries and IBM S/390 (31-bit)	
	9 for x86 (64-bit)	
	9 for x86 (32-bit)	
	9 for PowerPC	
	9 for EMT64 and AMD64	Service Pack 3 for pSeries
	9 for IBM iSeries/pSeries (64-bit)	
	8 for x86 (32-bit)	

Table 3. Supported platforms for servers, databases, and catalog manager (continued)

Platform		
Operating system	**Version**	**Level, service packs, patches**
Sun Solaris	10 Operating System for SPARC platforms	**Note:** Limitation to the deployment of agents on Solaris x86 platforms (global and non-global zones) is the following: Agents cannot be deployed on hardware that supports hyper-threading functionality.
	9 Operating System for SPARC platforms (32-bit)	

Agent and endpoint platforms

Table 4 lists the platforms supported for the agent.

Table 4. Supported agent and endpoint platforms

Platform		
Operating system	**Version**	**Levels, service packs, patches, compatibility packs**
Windows	Server 2003 Standard or Enterprise Edition (32-bit)	
	Server 2003 Standard or Enterprise Edition (64-bit) on EMT64 and AMD64	
	2000 Advanced Server (32-bit)	Service Pack 3
	2000 Server (32-bit)	
	2000 Professional (32-bit)	
	XP Professional	
	Vista for EMT64 and AMD64 x86	
	Vista for zSeries® and Intel x86 (32-bit)	
IBM AIX®	6.1	
	5.3 (32-bit)	xlC.aix50.rte.6.0.0.3 or later APAR IY51805 **Note:** For 64-bit platforms only: • Option 13 of 5722SS1 • Option 20 of 5722SS1
	5.3 (64-bit)	
	5.2 (32-bit)	
	5.2 (64-bit)	

Table 4. Supported agent and endpoint platforms (continued)

Platform		
Operating system	**Version**	**Levels, service packs, patches, compatibility packs**
i5/OS® (OS/400®)	V5R3	Option 13 and 20 of 5722SS1 PTF MF34223 to support sub capacity pricing on Power 5
	V5R2	Option 13 and 20 of 5722SS1 The following PTFs for product 5722SS1: SI10060, SI07110, 5722SS1 If the agent is running WebSphere Application Server, product 5722AC3 and PTFs SF99245, SF99169 If you intend to implement SSL between the runtime server and the agent, PTFs MF31411, SI10035, SI10759 SI17306, SI17781, SI20675
HP-UX	11i v1 on PA-RISC 2.0 64-bit	Patch PHSS_35381
	11i v2 on PA-RISC 2.0 32-bit	Patches: PHSS_26946, PHSS_33033
	11i v2 on PA-RISC on rx7640 and rx8640	Patches: PHSS_35381, PHSS_33033
	11i v2 on PA-RISC 2.0 64-bit (in 32-bit compatibility mode)	Patches: PHSS_26946, PHSS_33033
	11iv2 on Itanium 2 integrity server	
	11iv3 PA-RISC	

Table 4. Supported agent and endpoint platforms (continued)

Platform		
Operating system	**Version**	**Levels, service packs, patches, compatibility packs**
Red Hat Enterprise Linux	version 5.0 for Power	
	version 5.0 for zSeries (64-bit)	
	version 5.0 for x86 (64-bit)	
	version 5.0 for x86 (32-bit)	
	version 5.0 for pSeries (64-bit)	
	version 5.0 for xSeries AMD64/EM64T (64-bit)	
	version 5.0 for xSeries (32-bit)	
	ES/AS/WS 4.0 for EM64T and AMD64	Compatibility packs: 1. libgcc-3.4.3-9 (32-bit) 2. compat-libstdc++ -33-3.2.3-47.3.i386.rpm (Must be installed in the specified order)
	version 4.0 for Power	
	ES/AS/WS 4.0 for Intel x86	Compatibility packs: compat-libstdc++ -33-3.2.3-47.3.i386.rpm
	ES/AS/WS 3.0 for Intel x86	Update 1, Update 3
	AS, version 4.0 for IBM iSeries® and pSeries® (64-bit)	Compatibility packs: 1. libgcc-3.4.3-9 (32-bit) 2. compat-libstdc++ -33-3.2.3-47.3.ppc.rpm (Must be installed in the specified order)
	AS, version 3.0 for IBM iSeries and pSeries (64-bit)	Update 1, Update 2
	AS, version 4.0 for IBM zSeries and IBM S/390® (31-bit) on 64-bit hardware	Compatibility pack: compat-libstdc++ -33-3.2.3-47.3.s390.rpm
	AS, version 3.0 for IBM zSeries and IBM S/390 (31-bit)	Update 1

Table 4. Supported agent and endpoint platforms (continued)

Platform		
Operating system	**Version**	**Levels, service packs, patches, compatibility packs**
SUSE Linux Enterprise Server	10 for Power	
	10 for IBM zSeries and IBM S/390 (64-bit) on 64-bit hardware	
	10 for IBM iSeries/pSeries (64-bit)	
	10 for x86 (64-bit)	
	10 for x86 (32-bit)	
	10 for EMT64 and AMD64	
	9 for Power	
	9 for x86 (64-bit) 9 for x86 (32-bit)	Service pack 1 to support subcapacity pricing on Power 5
	9 for EMT64 and AMD64	
	9 for IBM iSeries/pSeries (64-bit)	
	9 for IBM zSeries and IBM S/390 (31–bit)	
	8 for PowerPC	
	8 for IBM zSeries	
Sun Solaris	10 Operating System for SPARC platforms (32-bit)	
	10 Operating System for SPARC platforms (64-bit)	
	10 Operating System for AMD64 and EMT64 (64-bit)	
	9 Operating System for SPARC platforms (32-bit)	
	9 Operating System for SPARC platforms (64-bit)	
	8 Operating System for platforms (32-bit) and (64-bit)	

Prerequisites

This section provides information about the prerequisites for the installation and operation of the license management extension.

Configuration Manager

The following are the prerequisites for Configuration Manager in the license management extension environment.

- IBM Tivoli Configuration Manager, Version 4.3.1. Specifically, ensure that the patches for the following components are installed:
  - Inventory
  - Inventory Gateway
  - Software Distribution Gateway
  - Software Distribution Server
  - Scalable Collection Services (MCollect)

To address interoperability between the License Compliance Manager DB2 administration server database and Configuration Manager inventory configuration manager Oracle database, WebSphere Information Integrator, Advanced Edition federated database technology is used. The following database versions are required for the database federation:

Table 5. Supported database versions of the Configuration Manager configuration repository database for the database federation

DB2
DB2 UDB, Enterprise Server Edition server, version 8.2
DB2 UDB, Enterprise Server Edition server, version 8.1.7
DB2 UDB, Enterprise Server Edition server, version 9.1 (only migrated, the first installation has to be performed with 8.2 or 8.1.7 versions because of prerequisites checking)

License Compliance Manager

The Configuration Manager license management extension involves the installation of only the following License Compliance Manager infrastructure elements:

- Administration server
- Administration server database
- Catalog manager

Note: Do not install the runtime server or runtime server database infrastructure elements. If you require a runtime server and database installation to manage agents to support sub-capacity licensing scenarios or virtualized environments, ensure that you install the runtime server and database on a dedicated computer where no other infrastructure element required by the license management extension is installed.

WebSphere Application Server is a prerequisite for the administsration server and DB2 UDB is a prerequisite for the administration server database. They are both packaged with License Compliance Manager. All of the prerequisites for these elements are fully documented in the *IBM Tivoli License Compliance Manager: Planning, Installation, and Configuration* and *IBM Tivoli License Compliance Manager: Release Notes*. Before installing License Compliance Manager, you must ensure IBM Tivoli Configuration Manager, Version 4.3.1 is installed on the required components. See “Configuration Manager” on page 16 for more information.

Prerequisites for new components

This section describes the requirements and considerations for individually installing the new license management extension components of IBM Tivoli Configuration Manager using Tivoli Management Framework, Tivoli Software Installation Service, or software packages.

The following Configuration Manager components are prerequisites for the Configuration Manager Extension for License Manager component:

- Inventory server
- Software Distribution server

This component must be installed first on the Tivoli server, and then subsequently on other managed nodes, provided that the node already has both the Inventory server and Software Distribution server components installed. It includes the installation of the License Compliance Manager Data Handler. The License Compliance Manager Data Handler can run on any managed node, but to avoid performance degradation, install the Configuration Manager Extension for License Manager on a computer different from the computer where the Inventory Data Handler. See Table 1 on page 7 for a description of this component.

Chapter 3. Preparing your Configuration Manager environment for the license management extension

This section describes how to install the license management components included in Configuration Manager.

IBM Tivoli Configuration Manager includes optional components that extend your environment to include license management capabilities.

Perform the following steps to prepare your Configuration Manager environment for the license management extension:

- Install Configuration Manager Extension for License Manager and Configuration Manager Endpoint Extension components. See “Installing and upgrading the license management extension components.”
- Run SQL scripts to create or update the Inventory database schema, and prepare your database for the federation. See “Preparing your databases for the federation” on page 24.

Before you start

Before you begin

To ensure a successful installation, perform these steps:

1. Plan the implementation of license compliance in your environment. See Chapter 2, “Planning the license management extension topology,” on page 7.
2. Check prerequisites as described in “Prerequisites” on page 16.
3. Back up the Configuration Manager configuration repository database.

Installing and upgrading the license management extension components

This section describes the license management extension components included in IBM Tivoli Configuration Manager.

The following license management extension components are included in IBM Tivoli Configuration Manager:

Configuration Manager Extension for License Manager
You install this component on the Tivoli management region server (Tivoli server) or a managed node. This component is located on the IBM Tivoli Configuration Manager CD in the path /NewComponents/EXTENSION/TLMEXT.IND.

Configuration Manager Endpoint Extension
You install this component on all gateways. This component is located on the IBM Tivoli Configuration Manager CD in the path /NewComponents/EXTENSION/CMEXT.IND.

To install the components, use the traditional Tivoli product installation methods. Refer to the *IBM Tivoli Configuration Manager: Planning and Installation Guide* for the installation procedure. Table 6 on page 20 provides the installation options that you specify when you install the components from either the command line interface

(CLI) or from the Tivoli desktop.

Table 6. Installation options for the Configuration Manager Extension for License Manager component

GUI Field name	CLI option
Description	
License Manager Administration Server address	@TLMServer@
The License Compliance Manager administration server address (IP address or host name).	
License Manager Extension Name	@TLMExtRTName@
The name of the License Manager Extension. The License Manager Extension allows the Administration server to recognize the Tivoli management region server as a License Compliance Manager runtime server. You need to provide this name when you install the License Compliance Manager administration server database.	
Catalog Manager user name	@CatManUser@
A user name with administrative rights to the DB2 database. You can log on as the `tlmsrv` user, which is created to enable the License Compliance Manager administration server to access the database, or as any other DB2 user that has read and write access rights to the SWCAT schema of the License Compliance Manager administration server database.	
Catalog manager password	@CatManPwd@
The password of the catalog manager user.	
Catalog manager installation parameter from CLI only	@FromTo@
When installing the Configuration Manager Extension for License Manager component with the **winstall** command, set this parameter to `CLI`. You include this parameter to indicate to the installation that the catalog manager password is not encrypted.	

The Configuration Manager Extension for License Manager is composed of the License Compliance Manager Data Handler and the License Compliance Manager handler. After you have installed this component, you can customize it in the following ways:

- Configure the License Compliance Manager handler settings by modifying the related parameters in the tlm_extension.ini file. This file is stored in the path $DBDIR/tlm_handler. See “The tlm_extension.ini configuration file” on page 83 for more information about this file.
- Start or stop the License Compliance Manager handler using the **wtlmhandler** command. See “wtlmhandler” on page 73 for the command syntax and usage of this command.
- You can change configuration parameters of the License Compliance Manager Data Handler such as, the debug level, the log size, and others, using the **wcollect** command. The License Compliance Manager Data Handler is another instance of the Inventory Data Handler that is customized to manage only License Compliance Manager data. You configure it just as you would the Inventory Data Handler. The License Compliance Manager Data Handler logs are stored in the path $DBDIR\tlm_data_handler. Refer to IBM Tivoli Configuration Manager: User’s Guide for Inventory for more information about the **wcollect** command and ways to configure the data handler.

Objects created by the installation

When you install the license management extension, it creates new objects in your Tivoli environment.

Table 7 lists the objects created by the installation:

Table 7. Objects created by the installation on the Tivoli desktop

Object	Name	Description
Policy Region	License_Management_<*TMR_region_name*>	Contains the TLMExtTaskLibrary task library and the ITLMInfoDistribution profile manager. This policy region is dedicated for the license management extension and is enabled for license management extension capabilities by default.
Task Library	TLMExtTaskLibrary	Contains a collection of tasks and jobs to download license management information to the agents installed on the endpoints.
Profile Manager	ITLMInfoDistribution	Contains the software packages used by the license management extension, and the Inventory scan profile, ITLMInventoryScan.
Tasks	RunTLMInfoGetDelta	Downloads the license management information from the administration server and pushes it to the agents by invoking the **wtlminfoget** command. Only a partial software catalog is distributed containing changes with respect to the preceding catalog distribution. For more information on the **wtlminfoget** command, see “wtlminfoget” on page 74.
	RunTLMInfoGetFull	Downloads the license management information from the administration server and pushes it to the agents by invoking the **wtlminfoget** command. The full software signature catalog is downloaded. For more information on the **wtlminfoget** command, see “wtlminfoget” on page 74.
	StartTLMExtension	Starts the Configuration Manager Extension for License Manager.
Jobs	RunTLMInfoGetDJ	Runs the RunTLMInfoGetDelta task. The results of the task are written to the $JOB_NAME.log file located in the $DBDIR/tlm_handler/log directory on the computer where the Configuration Manager Extension for License Manager is located. This job is disabled by default.
	RunTLMInfoGetFJ	Runs the RunTLMInfoGetFull task. The results of the task are written to the $JOB_NAME.log file located in the $DBDIR/tlm_handler/log directory. This job is disabled by default.
	StartTLMExtJob	Runs the StartTlmExtension task. This is enabled by default.

Table 7. Objects created by the installation on the Tivoli desktop (continued)

Object	Name	Description
Software Packages	ITLMInfo.1	This package is distributed to agents installed on endpoints and contains license management information such as, the software catalog, division information, agent information, and agent configuration. The **wtlminfoget** command prepares this software package and distributes it. For more information on the **wtlminfoget** command, see “wtlminfoget” on page 74.
	stopITLMAgent.1	This package is used to stop the License Compliance Manager agent. The collection of agent data is temporarily suspended. It also unregisters the agent as a service.
	startTLMAgent.1	This package is used to register and start the License Compliance Manager agent service.
Inventory profile	ITLMInventoryScan	This new profile is created in the dedicated license management extension policy region, License_Management_<*TMR_region_name*>. By default, it is configured to run only a hardware scan on the endpoints. Modify this profile to scan for installed software using signature matching. In this way, a corresponding License Compliance Manager software scan is automatically triggered to maintain information synchronized between the two databases. If you do not modify the profile, you cannot generate a License Compliance Manager report for scanned software. Inventory profiles can be configured from the Inventory Administrative graphical user interface or by using the **wsetinvpcsw** and **wsetinvunixsw** commands. Refer to the *IBM Tivoli Configuration Manager: User’s Guide for Inventory*.

If any of the objects created by the installation are accidentally deleted from your environment or if, for any reason, you need to restore this environment, see “Restore the Tivoli objects in the environment” on page 88.

Enabling the license management extension in your Tivoli environment

This topic describes how you can enable license management extension capabilities in your Tivoli environment.

After installing the Configuration Manager Extension for License Manager component, the License_Management_<*TMR_region_name*> policy region is created automatically and is enabled for license management extension capabilities by default.

The **inv_tlm_enabled** parameter, managed by the **winvmgr** command, is used to enable and disable license management extension capabilities. This parameter can be set on specific policy regions, and on the entire Tivoli environment. Policy regions in the same Tivoli management region can have different settings to achieve different types of behavior. All inventory profiles created in a profile manager that is associated to a policy region with license management extension capabilities enabled, are treated in the same way. The inventory profile distributed to perform a scan on an endpoint determines whether license management extension is applicable to that endpoint. To manage parts of your environment with license management extension capabilities and parts without these capabilities, you must carefully assign your inventory profiles to the appropriate profile manager and policy region.

After the installation of the Configuration Manager Extension for License Manager component, the behavior of the following functions changes as follows:

Inventory scans

The behavior is controlled at policy region level from where the inventory profile scan is created. If the ITLMInventoryScan has been modified to perform a scan for installed products using signature matching, then when the inventory profile scan is invoked from a policy region that is enabled for license manager extension capabilities, a License Compliance Manager software scan on the agent is automatically triggered so that the installed software information is always synchronized between the Configuration Manager configuration repository database and the License Compliance Manager administration server database. You can modify the ITLMInventoryScan Inventory profile to scan for installed products using signature matching from the Inventory Administrative graphical user interface or by using the **wsetinvpcsw** and **wsetinvunixsw** commands. Refer to the *IBM Tivoli Configuration Manager: User's Guide for Inventory*.

An inventory profile scan invoked from a policy region that is not enabled continues to be independent from the License Compliance Manager scan and the endpoint scan results are uploaded only to the Configuration Manager configuration repository database.

Signature management

When the license management extension is enabled in any policy region or on the Tivoli region, the License Compliance Manager signature format is used under the control of the catalog manager. You can continue to use both the **winvsig** command and software packages containing signature definitions to add signatures to the database, but you must ensure that the catalog manager is installed in the Tivoli environment on the computer where you will run the **winvsig** command. Signature management is returned to the control of Configuration manager only if all policy regions and the Tivoli region have the license management extension disabled.

Enabling and disabling license management extension capabilities

Before you begin

You can enable or disable license management extension capabilities at both the policy region level and at the Tivoli management region level. If you enable the Tivoli management region, all policy regions that it contains inherit the same setting, unless the policy region is explicitly disabled.

About this task

The following examples demonstrate how you can enable and disable license management extension capabilities at policy region level, and how you can enable the capabilities at Tivoli region level:

Example

- If in an environment with ten policy regions you want to only enable license management extension capabilities for endpoints subscribed to one policy region, PR1, submit the following command:

  ```
  winvmgr -c inv_tlm_enabled=y -p PR1
  ```
- To enable license management extension capabilities for the whole Tivoli region, with the exclusion of one policy region contained in the Tivoli region, PR9, submit the following command:

  ```
  winvmgr -c inv_tlm_enabled=y
  ```

  and then subsequently, submit the following command:

  ```
  winvmgr -c inv_tlm_enabled=n -p PR9
  ```

  By default, all other policy regions in the Tivoli management region, with the exception of the License_Management_<TMR_region_name> policy region, do not have a **inv_tlm_enabled** parameter setting and, therefore, they inherit the value of the parameter at the Tivoli management region level. Refer to IBM Tivoli Configuration Manager: User's Guide for Inventory for the syntax and usage of the **winvmgr** command.

Preparing your databases for the federation

This section describes the steps you need to perform to prepare your databases for the federation.

Before you begin

After installing Configuration Manager, perform the following tasks on the computer where the Inventory Server component is installed to prepare the Configuration Manager configuration repository database for the federation:

1. Ensure that you have updated Inventory signatures and packages with the latest IBM software catalog, if you have not already. To do this, perform the following steps:
   a. Verify that you have updated the inventory database schema using the scripts documented in *IBM Tivoli Configuration Manager: Planning and Installation Guide*. These scripts are copied to the managed nodes when the Configuration Manager Inventory server component is installed. Refer to *IBM Tivoli Configuration Manager: Planning and Installation Guide* for more information.
   b. Download the latest IBM software catalog file and run the **winvmigrate** command as follows: `winvmigrate -c` *`IBM_software_catalog_file`*, where *IBM_software_catalog_file* represents the IBM software catalog in XML format. A copy of the catalog is copied to the following path when you install the Configuration Manager Inventory component: *$BINDIR*/../generic/inv/SIGNATURES/IBM_SoftwareCatalog.xml. Before using this file, compare this file with the latest version available from the product support web site and use the most recent version.

      To verify if you have already run the **winvmigrate** command, check that the value of the TCM_DB_MIGRATED field is `YES` in the CONTROL table in the Configuration Manager configuration repository database.
2. Enable the database federation. Depending on whether the Configuration Manager inventory configuration repository database is DB2 or Oracle, run the appropriate script on the computer where the Configuration Manager configuration repository database is located to enable the database federation

between the License Compliance Manager administration database and the Configuration Manager configuration repository database. The installation of the Configuration Manager Extension for License Manager installs the `inv_ora_fed_schema.sql` and `inv_db2_fed_schema.sql` scripts in the following path on the Tivoli server: *$BINDIR*/TME/TLM_EXT/SCRIPTS.

Chapter 4. Installing License Compliance Manager

To implement the license management extension for Configuration Manager, you need only to install some of the License Compliance Manager infrastructure elements.

Before you begin

The Configuration Manager license management extension is not a full implementation of License Compliance Manager and, therefore, you do not need to install all infrastructure elements of the product.

About this task

You must install the following to use the license management capabilities of the extension:

- Catalog manager, version 2.3 fix pack 4
- Administration database, version 2.3 fix pack 4
- Administration server, version 2.3 fix pack 4

Results

These elements are installed in preparation for the Configuration Manager license management extension. Do not use the product such as create divisions, create organizations, or deploy agents.

Note: Do not install the runtime server or runtime server database infrastructure elements. If you require a runtime server and database installation to manage agents to support sub-capacity licensing scenarios or virtualized environments, ensure that you install the runtime server and database on a dedicated computer where no other infrastructure element required by the license management extension is installed.

Installation instructions for installing these infrastructure elements are documented in the *IBM Tivoli License Compliance Manager: Planning, Installation, and Configuration*. Specific Configuration Manager license management extension information is required for the administration server and database installation, see "Installing the license manager extension support" on page 28.

What to do next

Before you start

About this task

Before you start the installation, do the following:

1. Plan the implementation of license compliance in your environment. See Chapter 2, "Planning the license management extension topology," on page 7.
2. Check prerequisites. Check that the computers on which you plan to install the License Compliance Manager infrastructure elements are supported platforms

and meet the installation prerequisites. See "Prerequisites" on page 16 and refer to *IBM Tivoli License Compliance Manager: Planning, Installation, and Configuration* for more detailed information.

3. If the Configuration Manager configuration repository database is an Oracle database, complete the following steps:
   a. Install the Oracle client on the same computer where the administration server DB2 database is installed. Refer to the Oracle technical documentation.
   b. Register the Configuration Manager configuration repository database locally to the Oracle client on the computer where the administration server database is installed. Refer to the Oracle technical documentation.
   c. Install WebSphere Information Integrator, Advanced Edition on the same computer where the administration server DB2 database is installed. The installation images can be downloaded from the IBM Tivoli License Compliance Manager support Web site http://www-306.ibm.com/software/sysmgmt/products/support/IBMTivoliLicenseManager.html.

      WebSphere Information Integrator is currently known as WebSphere Federation Server, and has previously been known as DB2 Information Integrator. Documentation can be found on the DB2 Information Center http://publib.boulder.ibm.com/infocenter/db2luw/v8//index.jsp.

Installing the license manager extension support

This section describes how you install License Compliance Manager with the support for the license management extension for Configuration Manager.

In the Configuration Manager license management extension, the following License Compliance Manager infrastructure elements must be installed in the following order:

1. Administration server database

   The installation of the database requires you to select the option to activate the Configuration Manager license management extension and to provide information that is used to locate the Configuration Manager configuration repository database and create the license management monitoring infrastructure. The installation reconciliates the software catalog, federates the databases, and starts the replication processes. This installation procedure is documented in "Preparing the administration server database for the license management extension" on page 29.
2. Administration server

   The installation of the server requires you to select the option to activate the Configuration Manager license management extension and proceeds with the installation of the server as documented in *IBM Tivoli License Compliance Manager: Planning, Installation, and Configuration*.
3. Catalog manager

   This tool is used to customize the catalog of products that can be monitored and to import periodic updates of the IBM catalog in order to maintain accurate monitoring. The installation procedure is fully documented in *IBM Tivoli License Compliance Manager: Planning, Installation, and Configuration*.

After you have installed these License Compliance Manager infrastructure elements, you can proceed to deploy agents in your environment, see Chapter 5, "Deploying and configuring agents," on page 33.

Preparing the administration server database for the license management extension

This section describes how you install the License Compliance Manager administration server database and the Configuration Manager license management extension support.

Before you begin

Ensure that you have performed the steps described in “Before you start” on page 27.

About this task

Follow these steps to install the License Compliance Manager administration server database for the Configuration Manager license management extension. The version of DB2 UDB that is delivered with License Compliance Manager can be installed by the wizard.

1. Log on to the computer where you want to install the administration server database as a user with administrative rights (Administrator on Windows platforms or root on UNIX® platforms).
2. Copy the License Compliance Manager server and database CD on the hard disk of the computer.
3. Start the installation launchpad. When you are ready to install, click **Install IBM Tivoli License Compliance Manager** and when the installation page opens, click **Install server and database components**. The wizard starts and requests you to select the language version of the wizard that you want to use.

   The initial panels include a welcome panel and the license agreement. You must select the radio button to accept the license agreement before you can proceed by clicking **Next**.
4. Accept the default installation location displayed or click **Browse** to select a different location. Select the option to activate the Configuration Manager license management extension. Click **Next**.
5. Select to install the **Administration server database** and click **Next**. The DB2 prerequisite panel is displayed.
6. Select the option to let the wizard install DB2 UDB and click **Next**. The wizard requests the information required for installing the DB2 UDB prerequisite.
7. Depending on the platform where you are installing, you are asked to supply the following information:

   Windows platforms
   Supply the following:

   IBM DB2 path
   The directory where DB2 is to be installed.

   Port The port on which DB2 will listen.

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

UNIX platforms

Supply the following:

IBM DB2 instance owner's path

The home directory of the instance owner of DB2 on this computer.

Port The port on which DB2 will listen.

DB2 instance owner and password

The DB2 instance owner and password pair for which an account can be created on this computer. The instance owner is able to perform administrative tasks, such as creating and dropping databases, for this instance of DB2. The password must conform to any local rules that are in force.

Click **Next**.

8. Define the base configuration parameters.

   a. Specify and confirm the password to be used by server processes to access the administration server database. During installation of the database, the user `tlmsrv` is created with a password set to this value. The password must comply with any local rules that are in force in your environment and can contain only the following characters: **A-Z, a-z, 0-9, +, -, *, |, =** Keep a note of this password. You must specify it again when you install the administration server.

   b. Type the name of the organization to which the License Compliance Manager agents will belong or accept the default organization name. This is the name displayed on the administration server Web UI and on several reports. The default organization is created automatically by the installation.

      Attention: The license management extension permits the creation of only one organization in your environment.

   c. Type the name of the default division. The default division is created for the specified organization in the administration server database. Initially, all License Compliance Manager agents are assigned to this division. See "Reassigning agents to divisions" on page 37 for information about how to change the division to which an agent is mapped.

   d. Type the License Manager Extension name. This is the name specified when you installed the Configuration Manager Extension for License Manager component included in IBM Tivoli Configuration Manager, Version 4.3.1. See "Installing and upgrading the license management extension components" on page 19. This component allows the Administration server to recognize the Tivoli management region server as a License Manager runtime server. You can retrieve the name by locating the value of the **tlm_runtime_name** parameter in the tlm_extension.ini file. See "The tlm_extension.ini configuration file" on page 83 for details about this file.

   Click **Next**.

9. Select the vendor and version number of the Configuration Manager configuration repository database. If you have selected a DB2 database, indicate if the database is remote or local. A remote database also requires you to provide the host name and port number of the computer where the remote Configuration Manager configuration repository database is installed.

   Click **Next**.

10. Based on the database vendor you selected, provide the following additional information about the Configuration Manager configuration repository database:

DB2	Oracle
DB2 instance name The login name of the instance owner. **Database name** The name of the inventory configuration repository. **Inventory RIM user name** The inventory RIM user. **Inventory RIM password** The password of the inventory RIM user.	**Service Name** The name required to locate the inventory configuration repository. Specify the Oracle System Identifier that refers to the instance of the Oracle database running on the server. **Inventory RIM user name** The inventory RIM user. **Inventory RIM password** The password of the inventory RIM user.

    Click **Next**. A summary panel displays the installation location, the list of features to be installed, and the amount of space required for the installation.

11. Check the information about the installation and ensure that you have enough space to complete the installation, taking into account that creation of temporary files might mean that at times more space is used than the total size shown. If the amount of space you have available is about the same as the total size, clear some space before proceeding.
12. When you are ready to install, click **Next**. The installation will now start.

    If you installing the DB2 UDB prerequisite, you will be prompted to specify the location of the installation image.

    Note: If you choose the Activate the Configuration License Manager Extension feature, the License Compliance Manager server installation fails.
13. When the installation completes successfully, a summary panel displays the installation tasks that were completed. Click **Finish** to exit from the wizard.

Results

The installation performed the following tasks:

- Installed the software prerequisite DB2 UDB, for the administration server database if it was not already installed.
- Installed the administration server database.
- Performed the database federation.
- Merged the Configuration Manager catalog with the License Compliance Manager catalog.
- Started the Apply and Capture federation services.
- Registered the organization name, the License Manager Extension Name, and the default division specified during the installation.

Attention: The DB2 database replica processes, Apply and Capture, must be manually restarted each time the administration server database computer is rebooted. For more information, see “Stopping and starting the replica processes” on page 52.

What to do next

You can now proceed to install the administration server and catalog manager. Refer to *IBM Tivoli License Compliance Manager: Planning, Installation, and Configuration*.

Migrating inventory data to the administration server database

You can migrate inventory data collected for your endpoints to the License Compliance Manager administration server database, even before associating your endpoints with License Compliance Manager agents.

The itcminventorymigrate.sh script, located in the path <*INSTALL_DIR*>/admin/db/db2, on the administration server database computer, creates a fictitious agent for each endpoint and populates the administration server database with any inventory data already collected for the endpoint. The Configuration Manager inventory data can then be accessed from the administration server Web user interface, only when the internal task InventoryBuilderTask has run. The frequency period of this task is one day. You can change this period by modifying the value of the productInventoryBuilderPeriod parameter in the system.properties file on the License Compliance Manager administration server. See Refer to *IBM Tivoli License Compliance Manager: Planning, Installation, and Configuration* for more information about this parameter.

The following rules apply:

- The endpoint platform must be a supported License Compliance Manager agent platform.
- The inventory data in the Configuration Manager configuration repository database must be sufficient to create the agent node structure.

Run the script on the administration server database computer as follows:

```
itcminventorymigrate.sh <user> <password>
```

where,

<*user*>
Specify a user with the necessary privileges to access the administration server database.

<*password*>
Specify the password of the user.

You will be prompted to enter the administration server database user ID and password. The script can be launched in the following ways:

Without specifying any parameters.
The script collects data for all endpoints with inventory data stored in the Configuration Manager configuration repository database.

Specifying a file containing a list of computer system IDs (COMPUTER_SYS_ID).
The script collects data for only those endpoints that correspond to the COMPUTER_SYS_IDs listed in the file specified. The file contains a list of COMPUTER_SYS_IDs, each specified on a separate line. The COMPUTER_SYS_ID is defined in the COMPUTER Inventory table.

Attention: The itcminventorymigrate.sh script is not supported on Linux for IBM z/Series and IBM S/390 endpoints.

Chapter 5. Deploying and configuring agents

This section describes how you deploy agents on the Tivoli endpoint computers that you want to monitor and how you configure them after deployment.

The following steps outline the tasks required to deploy agents in your environment and prepare them for use. For information about managing agents that are up and running, see Chapter 7, “Managing agents,” on page 45.

1. Deploy agents. The following methods are available to deploy agents in your Tivoli environment:
   - Distribute an operating system specific software package to the endpoints on which you want to install the agent. See “Deploying agents using software package blocks.” This method is a more gradual deployment process comprised of several sub-steps that split the load of data flow in phases. To further minimize data flow, you can also plan this deployment method on small groups of endpoints at a time, rather than one single distribution targeting a large group of endpoints.
   - Distribute the ITLMInventoryScan inventory profile that is automatically created in the License_Management_<TMR_region_name> default policy region created at installation time. See “Deploying agents using inventory dependencies” on page 35. This method involves a single bulk transfer of data flow.
   - Run a wizard to update and prepare agents on i5/OS for the license management extension. See “Deploying i5/OS agents (OS/400)” on page 37.

   To avoid overloading the gateway collectors, you should use the software package distribution method.
2. Immediately after the agent installation, distribute the IBM software catalog, division information, agent information and agent configuration information to the agents using the **wtlminfoget** command. This is a Configuration Manager license management extension command. See “wtlminfoget” on page 74 for the command syntax and usage.
3. Organize agents into logical divisions by creating new divisions and reassign agents from the default division to the new divisions. See “Reassigning agents to divisions” on page 37
4. Update the division changes for the agents by distributing division information, agent information, and agent configuration information from the License Compliance Manager administration server to the agents by submitting the Configuration Manager license management extension **wtlminfoget** command. See “wtlminfoget” on page 74 for the command syntax and usage.

Deploying agents using software package blocks

You can deploy the License Compliance Manager agents to endpoints, using the software distribution functions of Configuration Manager.

Before you begin

This method of installation is preferred, if your environment contains low speed or unreliable connections. You must also use this method of installation if you want to convert a License Compliance Manager agent to a license management extension agent. The software packages are configured with a default variable that forces the installation of the license management extension agent on the classic License Compliance Manager agent.

Note:

- For i5/OS platforms, install the os400agent_tcm_enabled.spb software package block following the instructions in this section. To deploy agents on i5/OS platforms using the wizard, see "Deploying i5/OS agents (OS/400)" on page 37.
- For Linux 390 endpoints, you cannot distribute the software package block with the default configuration parameters. Refer to the appendix in *IBM Tivoli License Compliance Manager: Planning, Installation, and Configuration* for information about software package configuration parameters specifically for Linux 390 platforms endpoints.

About this task

Software packages for each supported agent platform are contained in the root path of the CD. Complete the following steps to distribute the agent installation code to the endpoints in your environment:

1. Ensure you have checked the prerequisites for this agent deployment method in the *IBM Tivoli License Compliance Manager: Planning, Installation, and Configuration*
2. Set up the Tivoli environment variables.
3. Ensure that you have distributed an Inventory profile from a policy region where the Configuration Manager license management extension is disabled to the endpoints where you want to install the License Compliance Manager agent code. The purpose of the Inventory profile distribution is to install the Common Inventory Technology (CIT) scanning technology and the Configuration Manager Endpoint Extension on the endpoints.
4. Copy the software package blocks required for this procedure from the CD to a directory on the Tivoli server or on another source host present in your Configuration Manager environment. The CD contains an agent installation SPB for each supported platform: <*platform*>_superspb.spb, where <*platform*> is one of the following values:
   - aix
   - hpux
   - linux
   - linux390
   - linuxppc
   - sun32
   - sun64
   - win32
5. Create a profile manager and a software package profile for each SPB that you want to distribute. Import the SPBs into the profile.
6. You can perform an install operation on the agent software package blocks using Software Distribution, specifying the appropriate platform-specific agent software package block named, <*platform*>_superspb.spb to each target computer. Distributions must be performed in undoable mode, using the force option.

Refer to the appendix in *IBM Tivoli License Compliance Manager: Planning, Installation, and Configuration* for a definition of the software package block and the possible values that can be assigned to each parameter.

7. Following the installation, perform an accept operation of the software package block and verify the change management state of the software package to confirm the success of the installation.
8. Run the **wtlminfoget** command specifying the all option to update the agent with agent information, the catalog, agent configuration data, and division information. See "wtlminfoget" on page 74 for the command syntax and usage. You can verify the success of this step by monitoring the ITLMInfo.1 software package using the **wmdist** command. This software package is produced each time you run the wtlminfoget command.

What to do next

The agent is installed in the *$LCF_DATDIR*/../../itlm file path. This path is not configurable.

See "Troubleshooting the installation" on page 77 and "Installation" on page 93 for troubleshooting and problem diagnosis information.

Deploying agents using inventory dependencies

You can deploy agents in your environment using the inventory profile, ITLMInventoryScan, created during the installation.

Before you begin

The License Compliance Manager agent can be automatically deployed on Tivoli endpoints when the ITLMInventoryScan inventory profile is distributed to the endpoints. This automatic installation mechanism is provided for each target platform supported by the license management extension, with the exception of OS/400 and Linux zSeries endpoints.

Note: Agent deployment on Linux zSeries endpoints is limited to the software package block distribution method. See "Deploying agents using software package blocks" on page 33.

About this task

You can use this method of agent installation if the following conditions exist:

- The operating system of the endpoint is supported by the License Compliance Manager agent. See "Supported platforms" on page 11 for supported agent platforms.
- Configuration Manager Extension for License Manager is installed on the Tivoli server. See "Installing and upgrading the license management extension components" on page 19.
- Configuration Manager Endpoint Extension is installed on the gateway to which the endpoint is connected. See "Installing and upgrading the license management extension components" on page 19.
- The Tivoli License Manager agent bundle component has been installed on the gateways connected to the endpoints where you want to install the agent code. This component copies the agent code to the gateway and a subsequent inventory profile distribution installs the agent code on the endpoints. The agent

code contains software package blocks that are downloaded to the endpoints each time an inventory scan is sent to the endpoints. An attempt is made to install the agent code or update the agent if necessary. If the agent is already installed on the endpoint, and no updates are necessary, then only the scan is performed.

- The endpoints on which you want to deploy agents are subscribed to profiles contained in policy regions with license management extension capabilities enabled. See “Enabling and disabling license management extension capabilities” on page 23.

If all the above conditions are met, the License Compliance Manager agent installation is automatically started on the endpoint. If you do not want to install the agent using this automatic installation mechanism, then you must disable the mechanism using the **winvdeps** command. Refer to the *IBM Tivoli Configuration Manager: User’s Guide for Inventory* for the command usage and syntax of the **winvdeps** command. If the installation finds a license management extension agent already installed on the endpoint, then it updates it. If, instead, it finds a classic License Compliance Manager agent installed, then the installation stops and a notice is sent to the Inventory notices group. If you want to upgrade a classic agent to a license management extension agent, see “Deploying agents using software package blocks” on page 33.

To deploy License Compliance Manager agents in your environment using an inventory profile distribution, complete the following steps:

1. Copy the Tivoli License Manager agent bundle index file from the CD to a temporary directory. The agent bundle index file (TLMAGT.IND) is contained in the \CDROM directory on the CD.
2. Install the Tivoli License Manager agent bundle component using the classic Tivoli product installation methods on all the gateways connected to endpoints where you want agents installed.
3. Distribute an inventory scan profile to the endpoints connected to the gateways where you installed the Tivoli License Manager agent bundle to install the agent. After the inventory scan is performed on the endpoints, the agent is installed and automatically starts.
4. Run the **wtlminfoget** command specifying the all option to update the agent with agent information, the catalog, agent configuration data, and division information. See “wtlminfoget” on page 74 for the command syntax and usage. You can verify the success of this step by monitoring the ITLMInfo.1 software package using the **wmdist** command. This software package is produced each time you run the wtlminfoget command.

What to do next

The agent is installed in the *$(LCFROOT)*/itlm file path. You cannot configure this path. If the installation fails, the inventory scan can still result as successful, but a warning message with an error code is issued in the Inventory Notices group. Refer to *IBM Tivoli License Compliance Manager: Problem Determination* for details about the installagent installation return codes.

See “Troubleshooting the installation” on page 77 and “Installation” on page 93 for troubleshooting and problem diagnosis information.

Deploying i5/OS agents (OS/400)

This topic describes deploying agents on i5/OS platforms in the license management extension environment.

Before you begin

You can deploy agents on i5/OS platforms using either a wizard or a software package block. The following procedure demonstrates using the wizard to deploy agents. See "Deploying agents using software package blocks" on page 33 for the procedure to deploy agents on i5/OS platforms using the os400agent_tcm_enabled.spb software package block located in the root path of the CD.

About this task

The i5/OS agent installation can be run interactively from a Windows computer that can connect to the i5/OS computer where the agent is to be deployed. To deploy a license management extension agent on i5/OS platforms using the wizard, complete the following steps:

1. Launch the setup file. Navigate to the following directory:

   ```
   <CD_drive>\setup\agent\OS400\Win32</CD_drive>
   ```

   Copy the `set up` directory to the C: drive of the computer.
2. Launch the set up file: `setupAgentOS400.exe`

   You are requested to sign on to the i5/OS computer.

   The wizard starts and requests you to select the language version that you want to install.

   After the welcome panel, select the option to install the Configuration Manager license management extension, and click **Next**.
3. A summary panel appears. Click **Next** to start the installation of the agent. When the installation is complete, click **Finish**
4. Run the **wtlminfoget** command specifying the all option to update the agent with agent information, the catalog, agent configuration data, and division information. See "wtlminfoget" on page 74 for the command syntax and usage. You can verify the success of this step by monitoring the ITLMInfo.1 software package using the **wmdist** command. This software package is produced each time you run the wtlminfoget command.

Reassigning agents to divisions

This section describes how you can assign an agent to a different division from the default division.

After you have installed and configured IBM Tivoli License Compliance Manager, you can perform tasks such as reassigning agents to logical divisions. For information about creating divisions, refer to *IBM Tivoli License Compliance Manager: Administration*.

When an agent is installed, a temporary division called DIV_CM is assigned to the agents. This is the default division name, but it can be configured during the installation. The first time an agent contacts the administration server to upload agent data, the agent is assigned to the default division.

You can organize your agents into logical divisions, in the same way as you can for profile managers. Agents you want to scan together should be in the same division. You can also group agents together for reporting or licensing purposes because some reports are produced at division level.

A command is available, **agtremap**, that you can use to assign the agent from the default division to a different division. When the agent has been assigned to a new division, you can no longer change this relationship.

Use the **agtremap** command to perform the following tasks:

- Reassign agents currently assigned to the default division, by specifying the agent ID, to a different division.
- Reassign agents currently assigned to the default division, by specifying the Tivoli endpoint Object ID (OID), to a different division. The command internally converts the Tivoli OID to an agent ID and assigns it to the target division. The License Compliance Manager administration server database table, ADM.AGENT_STATUS, provides a unique association between agent ID and Tivoli OID.

See "agtremap" on page 69 for the command syntax and examples.

The command requires an XML input file that specifies the reassignments, and a document type definition (DTD) file that is copied to the path, *<INSTALL_DIR>*\admin\SLM_Admin_Application.ear\slm_admin.war\webdoc\xml\import\agentRemappings.dtd, after the installation of License Compliance Manager on the administration server. You must customize the XML input file to include information about target divisions and agent IDs or Tivoli OIDs, or both. Both the input file and the DTD must be located in the same folder when you run the command.

The information required for the XML input file can be obtained from the ADM.AGENT_STATUS and ADM.DIVISION tables in the administration server database. Table 8 lists the columns in the table that contain the required information.

Table 8. Columns and tables containing the XML file information

XML file information	Column name, table
agent ID	**agent_id** , ADM.AGENT_STATUS
division ID	**division_id**, ADM.AGENT_STATUS
Tivoli OID	**endpoint_oid**, ADM.AGENT_STATUS

The following is a sample XML input file that contains instructions to remap agents, according to their ID, to a division, specifying the division ID. It also contains instructions to remap agents, according to their Tivoli OIDs, to different divisions:

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE agentRemappings SYSTEM "agtRemappings.dtd">
<agentRemappings>
 <agentRemapping>
  <targetDivision>99900000000001</targetDivision>
  <remappablesType>agent</remappablesType>
  <remappablesIDs>
   <remappablesID>100000000000000001</remappablesID>
   <remappablesID>100000000000000002</remappablesID>
   <remappablesID>100000000000000003</remappablesID>
     </remappablesIDs>
 </agentRemapping>
```

```
<agentRemapping>
  <targetDivision>99900000000009</targetDivision>
  <remappablesType>agent</remappablesType>
  <remappablesIDs>
   <remappablesID>900000000000000001</remappablesID>
   <remappablesID>900000000000000002</remappablesID>
    </remappablesIDs>
 </agentRemapping>
<agentRemapping>
  <targetDivision>99900000000001</targetDivision>
  <remappablesType>tme</remappablesType>
  <remappablesIDs>
   <remappablesID>tivoli_oid_100000001</remappablesID>
  </remappablesIDs>
 </agentRemapping>
<agentRemapping>
  <targetDivision>99900000000002</targetDivision>
  <remappablesType>tme</remappablesType>
  <remappablesIDs>
   <remappablesID>tivoli_oid_200000001</remappablesID>
  </remappablesIDs>
 </agentRemapping>
</agentRemappings>
```

For example, the agents with IDs:

```
100000000000000001
100000000000000002
100000000000000003
```

currently assigned to the default division, will be remapped to the division with ID 99900000000001.

While the Tivoli endpoint with ID tivoli_oid_100000001, currently assigned to the default division, will be remapped to division with ID 99900000000002.

After running the agent remap command, submit the **wtlminfoget** command on the endpoints for which the division has been changed, specifying the agent_info option to update the agent with the new division name. See “wtlminfoget” on page 74 for the command syntax and usage.

Chapter 6. Updating the License Management Extension

This procedure describes how to update the License Management Extension from a previous version to a more updated version of both products.

About this task

Updating the License Management Extension involves installation and configuration activities on some Configuration Manager components, and installation activities on some License Compliance Manager infrastructure elements.

Updating License Compliance Manager

Before you begin

The procedure for updating the License Compliance Manager infrastructure elements is essentially the same for the administration servers, databases, and the catalog manager. When the setup wizard is run on a computer where a previous version of a License Compliance Manager server or database is installed, the wizard automatically runs in upgrade mode. It upgrades the servers or databases that it detects, requesting any information that is needed for new or changed product features.

About this task

Follow these steps to update any of these infrastructure elements:

1. Log on to the computer where you want to run the installation as a user with administrative rights (Administrator on Windows platforms or root on UNIX platforms).
2. If you are upgrading a database for which the server is installed on a different computer, stop the server before continuing.
3. If you are upgrading a database, use the DB2 utilities to perform a backup of the database.
4. Launch the setup file for the administration server, database, or catalog manager for the platform where you are performing the update. The wizard starts. The initial panels include language selection and a welcome panel. Click **Next**.
5. The next panel enables you to select the backup location. Accept the default location displayed or click **Browse** to select a different location.

   The location must not be within the installation structure of any of the License Compliance Manager elements that are installed on the computer. The backup cannot be made in a directory that already contains files, so the directory you specify must either not yet exist or be empty.

   Click **Next**.
6. If you updating the administration server database, you are prompted to supply the password for the `tlmsrv` user that is used by the administration server processes to access the administration server database.

   Click **Next**.
7. Check the information about the installation and ensure that you have enough space to complete the installation, taking into account that creation of

temporary files might mean that at times more space is used than the total size shown. If the amount of space you have available is about the same as the total size, clear some space before proceeding.

8. When you are ready to install, click **Next**. The installation will now start.
9. When the upgrade completes successfully, a summary panel opens showing the upgrade tasks that were completed. Click **Finish** to exit from the wizard.

What to do next

You can now proceed to update your agents, see “Updating agents.”

Updating agents

This section describes updating agents that were deployed with a previous version.

About this task

The following methods are available to update agents in your Tivoli environment.

- Distribute an operating system specific software package to the endpoints on which you want to install the agent.“Updating agents using Configuration Manager software package blocks.”
- Distribute the ITLMInventoryScan inventory profile that is automatically created in the License_Management_<TMR_region_name> default policy region created at installation time.“Updating agents using inventory dependencies” on page 43
- Run a wizard to update and prepare agents on i5/OS for the license management extension. “Updating i5/OS agents (OS/400)” on page 44.

Updating agents using Configuration Manager software package blocks

You can update the License Compliance Manager agents on endpoints, using the software distribution functions of Configuration Manager.

Before you begin

This method of upgrade is preferred, if your environment contains low speed or unreliable connections.

About this task

Software packages for each supported agent platform are contained in the root path of the CD. Complete the following steps to distribute the agent update code to the endpoints in your environment:

1. Set up the Tivoli environment variables.
2. Ensure that you have distributed an Inventory profile from a policy region where the Configuration Manager license management extension is disabled to the endpoints where you want to install the License Compliance Manager agent code. The purpose of the Inventory profile distribution is to update the CIT on the endpoints, if necessary. If the CIT version is already up-to-date, no operation is performed.
3. To clean the objects that were created on your Tivoli desktop when you first deployed the agent with the previous release, perform these steps. On the Tivoli server, locate the agt_install.pl script provided with the License

Compliance Manager fix pack which you used to originally deploy agents in the Configuration Manager license management extension.

4. Run the script as follows:

   ```
   perl agt_install.pl -uninst
   ```

   where,

   -uninst
   : Removes from the Tivoli region the objects created when you ran the script to originally deploy agents. The following is the list of objects you remove by running the script:
     - The ITLM_Manager_<*region_name*> policy region.
     - The profile managers for each platform with the name ITLM_Agt_Deploy._<*platform*>.
     - The profiles for each of the software package blocks.
5. Copy the software package blocks required for this procedure. The installation image contains an agent installation SPB for each supported platform: <*platform*>_superspb.spb, where <*platform*> is one of the following values:
   - aix
   - hpux
   - linux
   - linux390
   - linuxppc
   - sun32
   - sun64
   - win32
6. Copy the software package blocks to a directory on the Tivoli server or on another source host present in your Configuration Manager environment.
7. Create a profile manager and a software package profile for each SPB that you want to distribute. Import the SPBs into the profile.
8. You can perform an install operation on the agent software package blocks using Software Distribution, specifying the appropriate platform-specific agent software package block named, <*platform*>_superspb.spb to each target computer. Distributions must be performed in undoable mode, using the force option. Refer to the appendix in *IBM Tivoli License Compliance Manager: Planning, Installation, and Configuration* for a definition of the software package block and the possible values that can be assigned to each parameter.
9. Following the installation, perform an accept operation of the software package block and verify the change management state of the software package to confirm the success of the installation.
10. Run the **wtlminfoget** command specifying the all option to update the agent with agent information, the catalog, agent configuration data, and division information. See "wtlminfoget" on page 74 for the command syntax and usage.

Updating agents using inventory dependencies

You can update agents in your environment using the inventory profile, ITLMInventoryScan, created during the installation.

About this task

To update License Compliance Manager agents in your environment using an inventory profile distribution, perform the following steps:

1. Ensure that the Tivoli License Manager agent bundle component is installed on all the gateways connected to endpoints where you want agents updated.
2. Install the agent bundle patch. The agent bundle update index file (TLMUPG.IND) is located in the /Upgrade directory on the CD.
3. Distribute the ITLMInventoryScan inventory profile to the endpoints connected to the gateways where you installed the agent bundle patch to update the agent.

What to do next

The agent is updated to the new version. If the update fails, the inventory scan can still result as successful, but a warning message with an error code is issued in the Inventory Notices group. Refer to *IBM Tivoli License Compliance Manager: Problem Determination* for details about the installagent installation return codes.

Updating i5/OS agents (OS/400)

This topic describes updating agents on i5/OS platforms in the license management extension environment.

Before you begin

On i5/OS computers, the agent cannot be redeployed while the original agent is present.

About this task

To update a license management extension agent on i5/OS platforms, you must uninstall the agent first. On this platform, uninstallation does not remove the agent configuration file. This file is retained in the /QIBM/UserData/QITLM directory and when the agent is reinstalled it is updated in the same way that the agent configuration file for distributed agents is updated during a redeploy; that is, the agent ID is not changed but parameters other than the organization can be changed. If you want to change the organization or the agent ID, you must remove the UserData directory before reinstalling the agent. For instructions on uninstalling the agent from an i5/OS computer, refer to *IBM Tivoli License Compliance Manager: Planning, Installation, and Configuration*.

What to do next

To update a license management extension agent on i5/OS platforms, complete the following steps:

1. Uninstall the current installation of the license management extension agent on i5/OS following the instructions documented in *IBM Tivoli License Compliance Manager: Planning, Installation, and Configuration*.
2. Deploy the new agent on the i5/OS computer using either the appropriate software package block, or the wizard. See “Deploying agents using software package blocks” on page 33 and “Deploying i5/OS agents (OS/400)” on page 37.

Chapter 7. Managing agents

This section describes how you can maintain the license management extension lifecycle.

You can manage your license management extension environment in the following ways:

- Maintain agents with up-to-date information such as the IBM software catalog, division information, agent information, and agent configuration information. See "Distributing information to the agents."
- Schedule a software scan to run, at intervals that you define, of the software installed on monitored computers. "How to schedule a software scan for a division" on page 46.
- Enable software products for monitoring. "How to enable products for monitoring" on page 47.
- Configure how information gathered on the agent is uploaded to the License Compliance Manager administration server. See "Transferring the extension component to a different location" on page 48.
- Start and stop the collection of agent data on request. See "Enabling and disabling agents using software packages" on page 48.

Distributing information to the agents

This section describes how the agents are updated with the IBM software catalog, division information, agent information, and agent configuration information.

You can update agents by distributing the IBM software catalog, division information, agent information, and agent configuration information from the License Compliance Manager administration server to the agents in the following ways:

Submit the RunTLMInfoGetFJ job

This job invokes the RunTLMInfoGetFull task. This task is created by default during the installation and is disabled by default. Invoking this task runs the run_wtlminfoget_full.sh script. This script invokes the **wtlminfoget** command to update the agent with a full catalog and update agent parameters. The requested information is packaged into a software package named, ITLMInfo.1, which is created in the ITLMInfoDistribution profile manager also created by the installation. By default, all endpoints subscribed to the ITLMInfoDistribution profile manager are targets of this task. You can customize the task to include other targets or modify what information is downloaded from the administration server. Customizing the task involves modifying the run_wtlminfoget_full.sh script stored in the path $BINDIR/TME/TLM_EXT/SCRIPTS, on the computer where the Configuration Manager Extension for License Manager is installed. You can also schedule the automatic repetition of this task using the Tivoli Scheduler.

You can also run the RunTLMInfoGetDelta task which runs the run_wtlminfoget_delta.sh script. This script invokes the **wtlminfoget** command to update the agent with a partial software catalog that contains only changes with respect to the last time the catalog was downloaded to the agent.See “Objects created by the installation” on page 21 for more information about these tasks, jobs, and the software package. Refer to *Tivoli Management Framework User’s Guide* for more information about jobs and tasks in general.

Run the wtlminfoget command
Run the **wtlminfoget** command on the computer where the Configuration Manager Extension for License Manager component is installed. You can invoke this command manually and specify the type of information you want to download to the agents. See “wtlminfoget” on page 74 for the syntax of this command.

You can submit the command or the job on an ad hoc basis to maintain the agent with up-to-date information.

You can modify the default agent behavior by modifying the agent configuration parameters in the agents_config.ini configuration file. See“The agents_config.ini configuration file” on page 86.

Note: When the computer system id is changed on an endpoint using the **wep** command, the Configuration Manager Endpoint Extension component does not consider the new system id until a new inventory scan profile is distributed to the endpoint. The agent gets updated with the new system id after the agent data is sent from the Tivoli management region through the **wtlminfoget** command. After the new scan, duplicate records in the inventory repository must be resolved to allow **wtlminfoget** to successfully start. Duplicate records are resolved by removing data for the old computer_system_ID using the **winvrmnode** command, or using the command **winvupdatecsid**.

How to schedule a software scan for a division

This topic describes scheduling a software scan from the License Compliance Manager Web interface for a division.

Before you begin

Information about installed software is collected from monitored computers by a deployed agent. Information is stored in a central DB2 database and can be accessed using the License Compliance Manager Web interface. You can schedule a scan for a specific division to run on the agents assigned to the division on a specific day and at a specific time, one time only, or to run at regular intervals.

About this task

Follow this procedure to schedule an installed software scan for a division:

1. Log on to the Web interface of the administration server.
2. In the portfolio, click **Schedule Software Scans**.
3. Filter for the division with which you want to work using the Division name field, and click **Search** to populate the divisions table.
4. Select a division from the table and click **Next**.
5. Define the scan date, scan time, and frequency.
6. Click **Finish**.
7. Submit the **wtlminfoget** command specifying the division_info option, and the targets, to update the agents with their scan schedule.

Results

The agents are updated with their scan schedule and will perform a software scan at the scheduled time. The scan results are sent up to the administration server database. When a License Compliance Manager scan runs, the upload manager invokes a Configuration Manager Inventory scan to maintain database synchronization between the two product databases.

How to enable products for monitoring

This topic describes how to enable a software product to detect its presence and use on a monitored computer. Information about software use is collected from monitored computers by the License Compliance Manager agent.

Before you begin

Monitoring software products that are installed and running on monitored computers enables the reconciliation of software use and installed software information with the license agreements for those software products.

About this task

Follow this procedure to enable monitoring for a product.

1. Log on to the Web interface of the administration server.
2. In the portfolio, click **Define Product Properties** → **Define Monitoring**.
3. Create a license and associate the license to the product you are enabling for monitoring.
4. Search for a product by completing the selection criteria, then click **Search**.
5. Select the products for which you want to define monitoring and click **Enable** to enable monitoring for the selected products.
6. Wait for the **catalogBuilderPeriod** to expire so that a new catalog is rebuilt by the administration server with the monitoring information. When a new catalog is generated, submit the **wtlminfoget** command indicating the **-**c DELTA option, and the targets of the command, so that a partial catalog is sent to the specified targets.

Results

The agents are now updated with the monitoring information and can begin monitoring the components associated to the software product that you enabled for monitoring. The presence and use information about the software product is uploaded to the administration server database.

What to do next

Note: If you want to enable monitoring for complex products, then you must first map the components of the products from the appropriate tasks on the administration server Web interface. Complex products are products, which are included in the catalog and can be monitored and assigned to licenses, that share a component with another product. This means that when the agent detects the component on a computer, it cannot automatically identify the product to which it relates. Refer to *IBM Tivoli License Compliance Manager: Administration* for information about mapping complex products.

Transferring the extension component to a different location

This section describes moving the Configuration Manager Extension for License Manager to a different location and how you can configure it.

You use the Configuration Manager Extension for License Manager to package the data files from the agents and send them to the administration server. Before the Configuration Manager Extension for License Manager sends the files to the administration server, it stores them in the depot directory and processes them.

You might need to transfer the Configuration Manager Extension for License Manager to a different managed node, for example, if you need to free up resources on the machine on which it is currently located. In this way, any data collected on the agent is redirected to the new location of the Configuration Manager Extension for License Manager which takes care of forwarding the agent data to the administration server.

Before moving the Configuration Manager Extension for License Manager to a different location, see “Prerequisites” on page 16 to ensure that the managed node to which you want to move the component has the prerequisites required.

Note: Ensure that an MDist2 repeater is present on the managed node where you want to transfer the Configuration Manager Extension for License Manager, otherwise, the **wtlminfoget** command does not work.

To transfer the Configuration Manager Extension for License Manager to a different location, complete the following steps:

1. On the managed node where the Configuration Manager Extension for License Manager is located, run the following command:

   ```
   wtlmdh -m managed_node
   ```

   where, *managed_node* represents the managed node to which you want to transfer the Configuration Manager Extension for License Manager.
2. After running the command, you must submit an inventory scan immediately to so that the agents are updated with the new location of the Configuration Manager Extension for License Manager.

   Note: To lessen the load of data on the infrastructure, you can submit a hardware scan instead of a software scan. Submitting a software scan might cause the accumulation of software data on the endpoint while it is in the process of resolving where to send the data. As a consequence, once the new location is resolved, the accumulated data is sent in one bulk transfer to the collector which can potentially overload it.

Enabling and disabling agents using software packages

This section describes how you can temporarily shut down a group of agents and then restart them.

Before you begin

You can temporarily suspend the collection of agent data by stopping the agents. It might be necessary to stop the agents if a communication error occurs between the administration server and the Configuration Manager Extension for License Manager. You can perform the operation on a subset of agents or on all agents by distributing a software package (stopITLMAgent) containing the License Compliance Manager command to stop the agent and disable the service. After installing the package, the agent is disabled. To re-enable the agent, you distribute a package containing the command to re-enable it (startITLMAgent) and restart the service.

About this task

To shut down a group of agents and then restart them when necessary, complete the following steps:

1. Distribute the stopITLMAgent software package located in the ITLMInfoDistribution profile manager to the endpoints where the agents you want to stop and disable are located. The collection of agent data is suspended on those endpoints and the agent services are no longer registered.
2. Perform whatever maintenance operations are necessary.
3. Register and restart the agent services by distributing the startITLMAgent software package to the endpoints where the agents to be restarted are located.

Chapter 8. Maintaining the federated databases

This section describes how you maintain the federated databases.

The License Compliance Manager administration server database and the Configuration Manager configuration repository database federation is based on the DB2 server instance capability of federating with DB2 or another vendor database server instance, such as, Oracle. When the database federation involves another vendor's database server instance, then you must install the WebSphere Information Integrator to enable the DB2 federation capabilities.

The database federation consists of components installed exclusively on the License Compliance Manager administration server database. Any customization of the database federation occurs on the administration server database where the federated components are installed and maintained. The database federation includes the following components:

The database wrapper and the related wrapping objects
This component is created at installation time and permits the administration server database to access remote instances of the Configuration Manager configuration repository database. It also creates a mapping between the local administration server database user and the user specified during the installation of License Compliance Manager for the remote Configuration Manager configuration repository database. The mapping is necessary to enable the replica processes to access the two databases.

The database replica tables
The database federation is based on the Structured Query Language (SQL) replica of the software catalog from the administration server database to the Configuration Manager configuration repository database. The SQL replica involves specific tables used by the replica processes to read and write the data changes. The replica tables are installed in the administration server database when the federation is setup during the installation.

The database replica processes
The SQL replica involves two processes that run on the computer where the administration server database is installed. The processes are:

Capture
This process reads any changes that occur on the administration server database from the transaction log and makes them available to the Apply process.

Apply
This process collects the data provided by the Capture process, and applies them to the Configuration Manager configuration repository database.

The replica processes are started at the end of the installation on the administration server database computer. As soon as they are started, they begin to replicate data from the administration server database to the Configuration Manager configuration repository database. When the database federation is being configured during the installation on the administration server database, the Configuration Manager configuration repository database software catalog is merged with the administration server software catalog to preserve the Configuration Manager data. The database federation consumes the Configuration Manager configuration repository database transaction log. To avoid filling up the transaction log, increase the size of the transaction log file size setting.

During the maintenance lifecycle of the federated databases, you might need to perform one or more of the following tasks:

- “Stopping and starting the replica processes”
- “Restoring a Configuration Manager configuration repository database backup” on page 53
- “Restoring a License Compliance Manager administration server database backup” on page 53
- “Configuring the data synchronization” on page 55
- “Modifying users and passwords” on page 55
- “Viewing logs and messages” on page 56
- “Reinstalling the federation” on page 56

With the installation of License Compliance Manager, several scripts are provided to aid you in performing these tasks. The scripts are located in the paths <*INSTALL_DIR*>/admin/db/db2 and <*INSTALL_DIR*>/admin/db/db2/federation on the administration server database computer.

Stopping and starting the replica processes

This section describes how to stop and start the replica processes.

You might need to stop and start the replica processes if a database problem occurs and you need to restore a backup, or if you need to perform routine maintenance operations on either the License Compliance Manager administration server database, the Configuration Manager configuration repository database, or both. Use the following scripts to stop and start the Capture and Apply processes on Windows computers:

- stopCapture.bat
- stopApply.bat
- startCapture.bat
- startApply.bat

Use the following scripts to stop and start the Capture and Apply processes on UNIX computers:

- stopCapture.sh
- stopApply.sh
- startCapture.sh
- startApply.sh

Note: You must be the DB2 administration server database instance owner to launch these scripts. By default, this user is defined during installation. On Windows, the default value for this user is Administrator, if this is the user performing the installation. If a user different from the user who installed the product needs to launch these scripts to start and stop the replica processes, then this user must have the necessary privileges to access the administration server database. You must also create a mapping between the administration server database user and the Configuration Manager configuration repository database user by modifying the setusrpsw.bat / setusrpsw.sh file. See “Modifying users and passwords” on page 55 for information about changing the value of the **TLM_DB_INSTANCE_OWNER** parameter with the name of the new administration server database user.

By default, the logs of the Apply and Capture services are stored on the administration server database computer in a service directory located in the path <*INSTALL_DIR*> / admin / db / db2 / federation / log. You can change this location by modifying the **SERVICE_LOG_DIR** parameter in the Apply and Capture start scripts. If you modify the **SERVICE_LOG_DIR** parameter, you must also update the scripts used to change passwords. See “Modifying users and passwords” on page 55.

Refer to the DB2 documentation Replica guide.

Note: The Apply and Capture replica processes must be restarted each time the administration server database computer is rebooted.

Restoring a Configuration Manager configuration repository database backup

When the Configuration Manager configuration repository database is federated with the License Compliance Manager administration server database, the software catalog is reconciled to maintain the information stored locally in the Configuration Manager configuration repository database. When a copy of the Configuration Manager configuration repository database is restored, the database administrator does not need to perform any steps to guarantee the consistency of the two databases. When the replication processes are started, the License Compliance Manager catalog is copied to the Configuration Manager catalog, restoring the Configuration Manager level of catalog which was stored in the administration server database.

Note: Stop the replica processes before restoring the Configuration Manager configuration repository database to avoid copying to the database when it is not available and restart them at the end of the restore process.

Restoring a License Compliance Manager administration server database backup

The administration server database maintains the master copy of the catalog. The replication processes copy the License Compliance Manager catalog to the Configuration Manager catalog. Before restoring a backup, the replica processes must be stopped to avoid a failure in attempting to accessing data locally, and to avoid erroneously copying data from the License Compliance Manager administration server database to the Configuration Manager configuration repository database. Also, stop the administration server database.

The procedure for the restore of the database depends on whether you have the transaction logs available. Follow these steps:

1. As a precaution, you can stop all agents and disable the service by distributing the stopITLMAgent software package to the agents. This avoids receiving a large number of trace errors that are generated by exceptions on the administration server until the process for restoring the database is complete.

These errors are not indication that the restore process is not working correctly. See "Enabling and disabling agents using software packages" on page 48.

2. Run the `db2 restore` command.
   - If the log files are not available run the command as follows:
     ```
     db2 restore db TLMA from <backup_path> without rolling forward
     ```
   - If the transaction logs are available, run the command as follows:
     ```
     db2 restore db TLMA from <backup_path>
     ```

     and then execute a rollforward operation to update the database with the latest information in the log files as follows:
     ```
     db2 rollforward database TLMA to end of logs and complete
     ```
3. When a backup is restored for the administration server database, some entries in the Configuration Manager catalog might be newer than those in the License Compliance Manager catalog. To avoid loss of Configuration Manager catalog entries, the two databases must be reconciled. The catalog reconciliation is performed using the following script located in the path <*INSTALL_DIR*>/admin/db/db2.

   Windows
   itcmcatmigrate.bat <*user*> <*password*>

   UNIX itcmcatmigrate.sh <*user*> <*password*>

   where,

   <*user***>**
   Specify a user with the necessary privileges to access the administration server database.

   <*password***>**
   Specify the password of the user.

   When you launch the script, you are prompted to enter the License Compliance Manager administration server database user ID and password. When the catalog reconciliation is complete, the replication processes can be started. A full replica of the software catalog data is performed from the License Compliance Manager administration server database to the Configuration Manager configuration repository database.
4. If a new catalog was downloaded to the agents during the period between the database backup and the database restore, then the server catalog will not be aligned with the catalog on the agents. Any data generated by the agents will not be processed correctly. To avoid this problem, manually update the ADM.SERVER table by changing the value of the **ADMIN_RECOVERY** parameter to 1 . This eliminates the catalog saved to the agent cache and discards the agent data until the catalog present on the administration server is downloaded to the agents.
5. Restart the replication processes.
6. Start the administration server so that a new catalog is generated.
7. To re-enable the agents and restart the service, distribute the startITLMAgent software package on the agents.
8. Run the **wtlminfoget** command on all the endpoints specifying the **agent_info**, and **catalog** options to update the agent with the correct information and the new catalog.

Configuring the data synchronization

You can configure the frequency with which table views are duplicated from the License Compliance Manager administration server database to the Configuration Manager configuration repository database. The default value is every 20 minutes. To change this value on DB2 navigate to **Control Centre** → **Replication Centre** → **SQL Replication** → **Definition** → **APPLY Control Servers** → **TLMA** → **Subscription Sets**. Modify the Subscription Set properties on the Schedule page.

Modifying users and passwords

The following scripts are provided for you to use if you are required to change the user and password used to access the Configuration Manager configuration repository database. This is the password and user name specified during the installation of the Configuration Manager license management extension.

Windows
setusrpsw.bat

UNIX setusrpsw.sh

The scripts create a mapping between the License Compliance Manager administration server user defined at installation time and the Configuration Manager configuration repository database user specified during the installation of the License Compliance Manager.

The administration server database users mapped to the Configuration Manager configuration repository database specified users are saved to the scripts with the following keys:

TLM_DB_INSTANCE_OWNER
The administration server database instance owner (the administrator, on Windows).

TLM_USER
The user defined to access data by the License Compliance Manager administration server.

If you modify the directory where database federation logs are stored by changing the value of the SERVICE_LOG_DIR parameter in the Apply and Capture start scripts, then you must also modify the script used to change the user and password. The REPLICA_FILE_PWD parameter must be changed so that the password file is created or updated in the new service directory.

Note: If the Configuration Manager configuration repository database is a DB2 server and the service directory is changed, then the replica processes cannot be started until the password file is restored. The password file can be restored by copying the replica.aut file located in the old path *<INSTALL_DIR>*/db/db2/federation/log to the new path. You can also restore the password file by running the script to change password with the required parameters as follows:

setusrpsw.bat *TCM_user TCM_user_password*

setusrpsw.sh *TCM_user TCM_user_password*

where,

TCM_user
: The Configuration Manager configuration repository database inventory RIM user name.

TCM_user_password
: The inventory RIM password.

Refer to *IBM Tivoli License Compliance Manager: Security Management* for information about changing License Compliance Manager passwords.

Viewing logs and messages

To view logs and messages related to the federated databases, you must enable the apply and capture services from **Control Centre** → **DB2 Replication Center** → **Capture Control Server** → **Apply Control Server**. Specify the following:

- Capture changes from the Master database (License Compliance Manager administration server database).
- Apply changes to the slave database (Configuration Manager configuration repository database).

You can also monitor the status of these services. If the apply service fails, an error message is logged in the trace file TCM_CAT_A.TRC in the path <*TLM_INSTALL_DIR*>/admin/db/db2/federation/log. This trace file is created the first time the apply service is started.

The log files of the apply and capture replica services are located in the path <TLM_INSTALL_DIR>/admin/db/db2/federation/log. See Table 21 on page 92 for more information about the log files.

Reinstalling the federation

The following set of scripts are copied at installation time that are configured to reinstall the federation in the case that a database restore of a previous backup becomes necessary:

Windows
: setupfed.bat

UNIX
: setupfed.sh

The script installs all the federation components, but does not start the replica processes.

You can edit the following parameters in the scripts to change the user mapping if required:

TLM_DB_INSTANCE_OWNER
: The License Compliance Manager administration server database instance owner (administrator, on Windows).

TLM_USER
: The user defined to access data by the License Compliance Manager administration server.

TARGET_USER_ID
: The Configuration Manager configuration repository database user.

Submit the script as follows:

```
setupfed.bat TCM_user_password
setupfed.sh TCM_user_password
```

where, *TCM_user_password* is the password of the Configuration Manager configuration repository database user saved to the **TARGET_USER_ID** parameter.

Chapter 9. Managing signatures

This section describes how you manage signatures in the integrated license management extension environment.

When your environment is set up to perform license management tasks, you can manage signatures using the License Compliance Manager catalog manager graphical user interface and command line interface. The signature information held in the catalog is the key to the capability of License Compliance Manager to accurately identify the products that start on monitored nodes so that their use can be monitored, and to recognize and accurately identify installed products on monitored nodes.

You can continue to manage signatures using the **winvsig** command. The behavior of this command changes depending on whether license management extension capabilities are enabled. See "Enabling the license management extension in your Tivoli environment" on page 22 for more details.

You can also continue to include signature definitions within a software package. See"Enabling the license management extension in your Tivoli environment" on page 22 for information about how this software package action is processed when the license management extension capabilities are enabled.

Signature tasks with catalog manager

This section describes how you use the catalog manager tool to expand and make changes to the list of products that can be monitored.

Use the catalog manager to do the following:

- Import updated catalog information from IBM.
- Set up software in hierarchical structures of products, versions, releases, and components.
- Associate executable files to components.
- Link signatures to product components.
- Integrate unknown executable files found running on monitored nodes with the catalog. These unknown files are discovered by the agent but are not linked to any product component. They represent an entity that potentially could be used to monitor software use if they are linked to existing product components or new components are created and linked to them.
- Add new products, change existing products, and disable products.
- Add new signatures or change existing signatures.

Attention: The catalog manager GUI is the preferred method for signature management and also offers more functionality. Refer to *IBM Tivoli License Compliance Manager: Catalog Management*for more information about using this tool.

Alternatively, you can manage signatures using the **winvsig** command. The **winvsig** command accesses the administration server database through the catalog manager. You can add, modify, or remove signatures using this command. In addition to the standard options available for this command, the -u and -p options are added for the Configuration Manager license management extension. These options are necessary to access the catalog manager.

If you import signatures that are not associated to components using the **winvsig** command, then a scan performed in an environment that is enabled for the license management extension does not discover these signatures. If you want to discover also those signatures, you must associate the signature to a new or existing component using the catalog manager.

Refer to *IBM Tivoli Configuration Manager: User's Guide for Inventory* for the standard command usage and syntax of the **winvsig** command. See "winvsig" on page 71 for the new options of the command related to the Configuration Manager license management extension.

Importing the catalog

Import the IBM Software Catalog to the Administration server database.

The IBM catalog is a knowledge base of product information that provides the information required by License Compliance Manager to recognize which products are installed and in use on monitored computers. IBM provides regular updates to the catalog and posts them on the support Web site.

You can import the catalog in several different ways:

- Catalog manager graphical user interface (GUI). Use the Import a New IBM Catalog task on the catalog manager GUI. Catalog manager enables you to manage conflicting entries. When a new IBM software catalog is imported, a check is made to discover any conflicting entries between the new catalog and the current database to avoid overwriting any changes made to the database since the last update. You can then select to either replace the existing entry with the entry in the IBM software catalog, or you can skip the replacement and maintain the existing entry in the database. Refer to *IBM Tivoli License Compliance Manager: Catalog Management*.
- **impcat** command invoked from the Administration server command line interface (CLI). Refer to *IBM Tivoli License Compliance Manager: Commands*.
- **catimp** command invoked from the catalog manager CLI. Refer to *IBM Tivoli License Compliance Manager: Commands*.
- **winvsig** command invoked from a managed node where the catalog manager is installed if the license management extension is already up and running in your Configuration Manager environment.

Downloading the catalog

Before you begin

To obtain the latest IBM software catalog, perform the following steps:

1. Access the latest catalog on the License Compliance Manager product support Web site: http://www-306.ibm.com/software/sysmgmt/products/support/IBMTivoliLicenseManager.html
2. Navigate the download pages to locate the latest catalog.
3. Download the relevant catalog files. Ensure that you do not download the catalog entitled ″for IBM software″.
4. Import the latest IBM catalog.

What to do next

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

Chapter 10. License management extension tasks

This section describes various license management extension tasks that you can perform.

The following are tasks you can perform when you have implemented the license management extension in your Configuration Manager environment.

- "Monitoring software use and installed software"
- "Monitoring and recognizing a potential signature" on page 64
- "Producing software use and software inventory reports" on page 67

Monitoring software use and installed software

You can monitor software use and installed software once you have implemented the Configuration Manager license management extension.

License Compliance Manager can provide you with the following types of information about the computers that you decide to monitor:

Installed software

You can use License Compliance Manager to perform scans at intervals that you define of the software installed on monitored computers. The installed software is detected and its product release level is identified.

The installed software scan is performed using the Common Inventory Technology software (CIT) that is also used by other Tivoli products for software recognition functions. The use of CIT enables scan results to be shared between Tivoli products, optimizing the use of system resources when multiple Tivoli applications are running on the same system.

You can also monitor installed software by configuring an Inventory profile to perform a scan for installed products using signature matching. If you configure the ITLMInventoryScan inventory profile to perform a scan for installed products using signature matching, then a License Compliance Manager software scan is also triggered so that the same set of installed software information is sent to each of the databases. Before you can verify the results of the software scan from the License Compliance Manager administration server Web interface, you must wait for the internal task, **InventoryBuilderTask**, to complete. By default this task is performed once a day. You can configure this period of time using the **productInventoryBuilderPeriod** parameter defined in the system.properties file. At this interval of time, the administration server reconciles the installed software information collected by the agent, which identifies the software components that are installed on monitored computers, with the product information stored in the administration server database.

Software use

The License Compliance Manager agent, deployed on a computer, collects information about use of software products. The agent is able to assemble information about the level and duration of use of a product. Level of use can be metered by number of users or number of processors. The metering unit to be used depends on the type of licenses that you define for your products. You can correlate software use with the license for the software if you set up license for the software product. To enable products for monitoring, see “How to enable products for monitoring” on page 47.

Both of these functions base their recognition of software products installed or in use on the information defined in the IBM software catalog.

For more information about monitoring software use and installed software, refer to *IBM Tivoli License Compliance Manager: Administration*.

Monitoring and recognizing a potential signature

This scenario describes how you associate a potential signature with a product component and enable recognition and monitoring.

Before you begin

This scenario assumes new divisions have been created other than the default division created by the installation.

About this task

The scenario describes the task of deploying agents in the Marketing profile manager, reassigning the agents to new divisions, enabling the potential signature files upload mechanism, processing the potential signatures, and mapping the potential signatures to components

1. Deploy and configure agents. See Chapter 5, “Deploying and configuring agents,” on page 33. The License Compliance Manager agents are registered on the License Compliance Manager administration server under the default division created at installation time.
2. Enable the potential signature files upload mechanism so that License Compliance Manager agents collect information about potential signatures that are identified while monitoring software usage. By default, the upload mechanism is disabled. To enable the mechanism, the following command must be submitted on all the endpoints subscribed to the Marketing profile manager.

   ```
   tlmagent –set unk y
   ```

   The tlmagent command is located in the path $LCF_DATDIR/../../itlm. You can either launch the command manually on each endpoint, or you can create and distribute a software package that runs the command on the endpoints automatically. To run the command automatically using a software package, complete the following steps:

   a. Create a new software package that includes an Execute program action and define the command in the software package action. To aid you in defining the software package that contains this action, you can use the stopITLMAgent.1 or startITLMAgent.1 software packages as a template. These software packages were created at installation time. The following is an excerpt of how the execute program action can be defined:

```
execute_user_program
               caption = "Enable unknown on agent HP/Sun/Linux/Win/AIX"
               condition = '($(os_name) == "HP-UX") OR ($(os_name) == "SunOS") OR ($(os_name) == "Linux")
OR ($(os_name) LIKE "Win*") OR ($(os_name)   ==  "OS400") OR  ($(os_name) == "AIX")'
               transactional = n

               during_install
                       path = $(root_dir.$(os_family))/$(itlm_install_dir)/tlmagent
                       arguments = "-set unk y"
```

```
        inhibit_parsing = n
        timeout = 120
        unix_user_id = 0
        unix_group_id = 0
        user_input_required = n
        output_file_append = n
        error_file_append = n
        reporting_stdout_on_server = n
        reporting_stderr_on_server = n
        max_stdout_size = 10000
        max_stderr_size = 10000
        bootable = n
        retry = 0

        exit_codes
                success = 0,0
                failure = 1,65535
        end

end
```

b. Distribute the software package on all the endpoints.

3. When the agent is monitoring software usage, if it discovers a signature but cannot find it in the catalog, then it cannot monitor the product. It adds the signature to the list of potential signatures, and these are passed to the administration server and stored in the database. Start the catalog manager and use the Register potential signatures task in the portfolio to link the signature to either a new product component or to an existing product component. The frequency with which potential signatures are uploaded is defined in the agents_config.ini file by the **uploadMinTime** parameter. By default, potential signatures are uploaded once a day. Refer to *IBM Tivoli License Compliance Manager: Catalog Management* for information about registering potential signatures. See "The agents_config.ini configuration file" on page 86 for information about modifying the **uploadMinTime**.
4. The next time the catalogBuilderPeriod expires, the administration server rebuilds the catalog containing any changes made to the catalog and the monitoring information. After the catalog has been rebuilt, submit the **wtlminfoget** command to the agents, specifying the **-c DELTA** option so that the agents are informed of which components to monitor.

Results

The signature can now be discovered and then, if enabled, monitored by the agent to measure software usage by the product component to which the signature is linked.

What to do next

To disable the potential files upload mechanism, run the command `tlmagent -set unk n`.

Restricting potential signature collection

Before you begin

The software use monitoring function of the agent includes the capability to collect information about software use signatures that are not included in the catalog. When the agent detects the starting of an executable file it attempts to match it to a product in the catalog. If the executable file does not match a catalog entry, the agent adds it to the list of potential signatures to be sent to the administration server, where they are stored in the administration server database and can be processed using the catalog manager tool.

This feature can cause performance problems when the agent is installed on a system where an application that generates a large number of transient executable files is running. In such a case, the agent and the administration server are forced to store and process very large numbers of potential signatures. In addition to the storage and performance problems this causes to the agent and administration server, it also populates the list of potential signatures that are unlikely to be added to the catalog. This reduces the usefulness of the potential signatures list.

About this task

You can create a file named, unknownFiles.properties, to define directories for which potential signature information is not of interest. The administration server rejects any signatures that were detected in one of the paths specified in this file and they are not included when potential signatures are sent to the administration server.

To create this file, follow these steps:

1. Create a Java™ properties file named unknownFiles.properties.
2. Define the following two properties in the file:

   windowsPathToSkip
   The relative paths that are to be excluded from unknown module monitoring on Windows systems.

   Note: Each backslash in the path must be doubled.

   unixPathToSkip
   The relative paths that are to be excluded from unknown module monitoring on UNIX systems. UNIX paths are case-sensitive.
3. For each property , you can define one or more relative paths that are to be excluded. You can list multiple paths by forming a concatenated string in which paths are separated by the “;” character. Multiple paths can also be included by using the “*” character as a wildcard. For example, to exclude the following locations on a Windows system:
   - C:\appdir30112006
   - C:\appdir01122006
   - C:\appdir02122006
   - \\.\GLOBALROOT\DEVICE\HARDDISKVOLUME1\TMP

   Include the following entry in the unknownFiles.properties file:

   ```
   windowsPathToSkip=C:\\appdir*;\\\\.\\GLOBALROOT\\DEVICE\\HARDDISKVOLUME1\\TMP:
   ```
4. Save the file to the following path: $INSTALL_DIR\admin\SLM_Admin_Application.ear\slm_admin.war\WEB-INF\conf.
5. Stop and restart the server to so that the changes take effect.

Note:

1. Each property can include one or more paths. Each path can be a directory or a drive.
2. To specify multiple paths, form a concatenated string within which the relative paths are separated by the character “;”.

3. The wildcard character “*” can be used in the definition of paths to be skipped.

Producing software use and software inventory reports

This topic describes querying the database to produce software use and software inventory reports.

Historical reports of inventory and software use information are available on the administration server. License Compliance Manager includes a set of reports with predefined queries for the analysis of collected software use and inventory data. You can view a report using the administration server Web interface as soon as the report has been generated, or you can choose to have a report generated through batch processing.

Reports can be produced in real time and viewed online or you can create a request and add it to the queue for batch processing. A batch reports status task is available, allowing you to check on the progress of batch requested that have been queued. When a batch report is ready, you can download it as an XML file.

Note: Sometimes, a report does not include products that you know are installed on monitored nodes. There is a time delay between the inventory scan and the availability of the new inventory information on the administration server. Before you can verify the results of the scan, you must wait for the internal task, **InventoryBuilderTask**, to complete. By default, this task is performed once a day. You can configure this period of time by modifying the value of the **productInventoryPeriodBuilder** parameter defined in the system.properties file.

The following reports are available:

Installed software snapshot
Provides a view of the products installed on monitored computers at a specified date and time. This is the same set of information that the ITLMInventoryScan inventory profile returns when it is configured to perform a scan for installed products using signature matching.

Product use level analysis
Provides a view of the level of use of products during a specified period. The report can be restricted to products with use above or below a specified level.

Product use trend analysis
Provides a graphical view of the trend in the use of a single selected product over time.

License use trend analysis
Provides a graphical view of the trend in the use of a single selected license over time.

License compliance
Provides a view of the license use situation at a specified time. The report shows the quantity available and percentage used for each license at the specified time. It also provides a high water mark value, indicating the highest level of use during a selected period leading up to the specified time. You can identify out of compliance situations and under-use of licenses.

Unlicensed use

Provides a view of the products that were used at a specified time for which no valid license was available.

Refer to *License Compliance Manager: Administration* for more information about the Web interface, requesting reports, and the roles required to request reports.

Chapter 11. Command reference

This section describes the command syntax and usage for commands used in the license management extension environment.

The following is a new License Compliance Manager agent command:

- **agtremap**

The following are Configuration Manager commands:

- **winvsig**
- **wtlmdh**
- **wtlmhandler**
- **wtlminfoget**

agtremap

Reassigns the agent to a division different from the original default division.

Purpose

Agents are assigned to a default division at installation time. Use this command to reassign the agent to a different division. The division must first be created from the administration server Web interface using the **Manage Organizations** task from the portfolio. The new division is specified using the division ID in an input XML file, and the agents are specified using either the Tivoli object identifier (OID) assigned to it or the agent ID.

agtremap *xml_file*

Parameters

xml_file
: The absolute path to the XML file containing the list of agent IDs and Tivoli OIDs to be remapped to different divisions. This file must be located in the same folder as the document type definition (DTD) file. The DTD file is copied to the path, $INSTALL_DIR/admin/SLM_Admin_Application.ear\slm_admin.war\webdoc\xml\import\agentRemappings.dtd. with the installation of the License Compliance Manager administration server infrastructure element.

Authorization

administrator or root

Return Values

The **agtremap** command returns one of the following values:

0	Indicates that agtremap ran successfully.
< > 0	Indicates that agtremap failed.

Examples

- To reassign an agent with agent ID 100000000000000001 to a division with a division ID of 99900000000001:

  ```
  agtremap c:\remap\remap.xml
  ```

  Note: The agentRemappings.dtd file must also be located in the same path as the remap.xml file.

  The following is an excerpt from the remap.xml file for this example:

  ```
   <agentRemapping>
    <targetDivision>99900000000001</targetDivision>
    <remappablesType>agent</remappablesType>
    <remappablesIDs>
     <remappablesID>100000000000000001</remappablesID>
    </remappablesIDs>
   </agentRemapping>
  ```

- To reassign an endpoint with Tivoli OID of tivoli_oid_100000001 to a division with a division ID of 99900000000001:

  ```
  agtremap c:\remap\remap.xml
  ```

  The following is an excerpt from the remap.xml file for this example:

  ```
    <agentRemapping>
    <targetDivision>99900000000001</targetDivision>
    <remappablesType>tme</remappablesType>
    <remappablesIDs>
     <remappablesID>tivoli_oid_100000001</remappablesID>
    </remappablesIDs>
   </agentRemapping>
  ```

- To reassign two agents with agent IDs of 828778589 and 13507270 to a division with a division ID of 12:

  ```
  agtremap c:\remap\remap.xml
  ```

  The following is an excerpt from the remap.xml file for this example:

  ```
    <?xml version="1.0" encoding="UTF-8"?>
  <!DOCTYPE agentRemappings SYSTEM "C:\Program Files\IBM\TLM\admin\
  SLM_Admin_Application.ear\slm_admin.war\
  webdoc\xml\import\AgentRemappings.dtd">
  <agentRemappings>
    <agentRemapping>
     <targetDivision>12</targetDivision>
     <remappablesType>agent</remappablesType>
      <remappablesIDs>
       <remappablesID>828778589</remappablesID>
       <remappablesID>13507270</remappablesID>
      </remappablesIDs>
    </agentRemapping>
  </agentRemappings>
  ```

  the output of the command is as follows:

  ```
  ITLCM Admin Server-CLI>agtremap C:\Software_Catalog\agtremap.xml
  CODCL0029I
  Number of files successfully processed: 1.
  Number of entities successfully processed: 1.
  The command was performed in 7 seconds.
  ITLCM Admin Server-CLI>
  ```

  where

  Number of entities successfully processed
  Indicates the number of agentRemapping tags present in the .XML file you provided in input.

winvsig

Modifies the password of the user with access to the catalog manager used by Inventory to access the catalog information stored in the License Compliance Manager database.

Syntax

winvsig -u *usesrname* [**-p** *password*]

Description

Important: The command syntax and usage of the standard options available for this command are described in *IBM Tivoli Configuration Manager: User's Guide for Inventory*. The -u and -p options are not included in the standard options for this command, but are available only with the Configuration Manager license management extension.

This command is used to change the password of the user with access to the catalog manager that connects to the database where the master catalog is stored. If the License Compliance Manager password used by the DB2 user is changed using the **dbpasswd** command, then use the **winvsig** command to change the password in the Configuration Manager environment.

Parameters

-u *username*
Specifies the valid user ID with access to the catalog manager database.

-p *password*
Specifies the password needed to access the catalog manager database.

Authorization

Refer to *IBM Tivoli Configuration Manager: User's Guide for Inventory*.

Return Values

Refer to *IBM Tivoli Configuration Manager: User's Guide for Inventory*.

Examples

To change the password of the tlmsrv user to tivoli, run the command as follows:

```
winvsig -u tlmsrv -p tivoli
```

wtlmdh

Creates or moves the Configuration Manager Extension for License Manager in the Tivoli management region.

Syntax

wtlmdh{ **-c** *managed_node* | **-m** [**-t** *timeout*] *managed_node* }

Description

This command operates only in the local Tivoli management region (Tivoli region). It is not possible to create or move the Configuration Manager Extension for License Manager across different Tivoli regions. Any change made to the Configuration Manager Extension for License Manager using this command requires a new Inventory scan submission to the endpoints. The purpose of the scan is to update the changes on the endpoint extension so that any data generated on the endpoints is correctly uploaded to the administration server. See "Prerequisites" on page 16 for the prerequisites of the Configuration Manager Extension for License Manager component before moving the component to another managed node.

Note: Ensure that an MDist2 repeater is present on the managed node to which you want to transfer the Configuration Manager Extension for License Manager, otherwise, the **wtlminfoget** command does not work.

Parameters

-c *managed_node*
Creates a new Configuration Manager Extension for License Manager on the specified managed node. If a License Compliance Manager Data Handler already exists in the environment, then the command fails. Only one instance of this object can be created for a single Tivoli region.

-m *managed_node*
Moves the Configuration Manager Extension for License Manager to the specified managed node. If the target managed node cannot be contacted, then the command fails.

-t *timeout*
The number of seconds after which the command will time out if it cannot contact the managed node to which you want to move the Configuration Manager Extension for License Manager. The default value is 60 seconds.

Authorization

senior or super

Return Values

The **wtlmdh** command returns one of the following values:

0	Indicates that wtlmdh ran successfully.
< > 0	Indicates that wtlmdh failed.

Examples

- To move the Configuration Manager Extension for License Manager to a managed node named jupiter, submit the following command:

```
wtlmdh -m jupiter
```

- To create the Configuration Manager Extension for License Manager on the managed node Jupiter because it was not properly created during installation, submit the following command:

```
wtlmdh -c jupiter
```

See Also

"wtlmhandler" on page 73

wtlmhandler

Starts and stops the License Compliance Manager handler which is a sub-component of the Configuration Manager Extension for License Manager component.

Syntax

wtlmhandler {**-h** *immediate* | **-h** *graceful* | **-s**}

Description

This command starts and stops the License Compliance Manager handler sub-component. You run this command from the computer where the License Compliance Manager handler is active. If the Configuration Manager Extension for License Manager component has not been transferred to a different computer since installation time, then it is located on the Tivoli server.

Parameters

-h *immediate* | **-h** *graceful*
Stops the License Compliance Manager handler sub-component in one of the following ways:

immediate
Stops the License Compliance Manager handler sub-component without waiting for active operations to finish processing. When you restart the component, any operations that were active when the component was halted are automatically restarted, so no data is lost.

graceful
Stops the License Compliance Manager handler sub-component after it completes all active operations.

-s Starts the License Compliance Manager handler sub-component again after it has been stopped. If it is already running, the command does nothing.

Authorization

admin, senior, super

Return Values

The **wtlmhandler** command returns one of the following values:

0	Indicates that wtlmhandler ran successfully.
< > 0	Indicates that wtlmhandler failed.

Examples

- To stop the License Compliance Manager handler sub-component without waiting for active operations to finish processing, submit the command as follows:

  ```
  wtlmhandler -h immediate
  ```

- To restart the License Compliance Manager handler sub-component and resume processing operations that were active and not completed when the component was stopped, submit the command as follows to restart the License Compliance Manager handler sub-component:

  ```
  wtlmhandler -s
  ```

See Also

"wtlmdh" on page 71

wtlminfoget

Run this command on the Tivoli server or on a managed node where the Configuration Manager Extension for License Manager is installed and enabled. This command assembles information into a software package on the Tivoli server and distributes it to agents.

Syntax

wtlminfoget [**-c** *FULL* | *DELTA*] {**-t** *target1,target2,...,targetN* **-T** *target_file* **-P** *profile_manager* }{ ALL | [*catalog*] [*division_info*] [*agent_info*] [*agent_config*] }

Description

This command retrieves information such as the IBM software catalog, division information, and agent information from the administration server, and agent configuration information. The information is then packaged into a software package named, ITLMInfo.1, and distributed to agents, each identified by the endpoint label on which the agent is located.

Parameters

-c *FULL|DELTA*
Specifies whether to distribute the entire IBM software catalog, or a partial catalog containing only the changes with respect to the last time the catalog was distributed. This parameter is used when either the ALL or catalog option is specified. In each of these cases, the default value FULL is assumed if the parameter is not specified.

FULL
Distributes the entire IBM software catalog.

DELTA
Distributes a partial catalog containing only changes with respect to the preceding catalog distribution. Only one partial catalog is created even if multiple targets are specified having different previous catalog distribution dates. The partial catalog is created using the earliest catalog distribution date among the selected targets.

-t *target1,target2,...,targetN*
Specifies the destination target of the distributed information. The target must be specified using the endpoint label. When specifying more than one target, the endpoint labels are specified separated by commas and with no blank spaces. The parameter can be specified more than once, and can also be used in combination with the -P and -T parameters. Duplicate targets are ignored.

-T *target_file*
Specifies to distribute the package to a list of endpoint labels specified in a file. The endpoint labels must be indicated one on each line. The parameter can be specified more than once indicating a different target file, and can also be used in combination with the -t and -P parameters. Duplicate targets are ignored.

-P *profile_manager*
Specifies to distribute the package to the targets subscribed to a specified profile manager. The parameter can be specified more than once indicating

targets subscribed to different profile managers, and can also be used in combination with the -t and -T parameters. Duplicate targets are ignored.

{ **ALL** | [*catalog*] [*division_info*] [*agent_info*] [*agent_config*] }
Indicates what type of information to include in the software package that is distributed to the specified targets. At least one information type must be indicated. More than one information type can be indicated separated by a blank space.

ALL
Indicates to include the following information in the software package: IBM software catalog, division information, agent information, agent configuration information.

catalog
Indicates to include the IBM software catalog in the software package.

division_info
Indicates to include division information in the software package. It contains the scan scheduling information for each division.

agent_info
Indicates to include agent information in the software package about only those agents identified as targets of the distribution. All other agent information is discarded. Use this option after the agent is first installed, when the agent is remapped to a division different from the default division, and when the administration server database is restored.

agent_config
Indicates to include agent configuration information in the software package. It includes the configuration information contained in the agents_config.ini file.

Authorization

admin, senior or super

A login for the root_user must be defined for the Tivoli Administrator of the managed node from where the command is invoked, and this same Tivoli Administrator must have the required authorization roles.

The senior or super role is required if the command-line interface must recreate the ITLMInfo.1 software package in the event that it was deleted.

Return Values

The **wtlminfoget** command returns one of the following values:

0	Indicates that wtlminfoget ran successfully.
< > 0	Indicates that wtlminfoget failed.

Examples

- To distribute the FULL catalog, division information, agent information, and agent configuration to the agents on endpoints with the following labels:“ myendpt” and “myendpt2”:

  ```
  wtlminfoget -t myendpt,myendpt2 ALL
  ```

- To distribute a partial IBM software catalog and division information to all targets specified in the file mytargets_file1.txt:

  ```
  wtlminfoget -c DELTA -T mytargets_file.txt catalog division_info
  ```

- To send the entire IBM software catalog, division information, agent information, and agent configuration to all targets subscribed to the ’pm’ profile manager, as well as to the endpoint ‘myendpt’:

  ```
  wtlminfoget  -P pm -t myendpt ALL
  ```

See Also

“wtlmhandler” on page 73

Chapter 12. Troubleshooting

This chapter provides an overview of the problem determination support available for the Configuration Manager license management extension.

Troubleshooting information is divided into the following categories:

- "Troubleshooting the installation."
- "Interrupting data flow to the administration server database" on page 79
- "Tuning" on page 79. Discusses ways you can tune or alter the default configuration of the Configuration Manager license management extension.
- "Traces and logs" on page 89.
- "Diagnosing problems" on page 93.

Troubleshooting the installation

This section provides information about verifying the installation, problems that might occur during the installation of the software, and information about performing recovery actions.

Before you begin

The steps to getting the Configuration Manager Extension for License Manager up and running are outlined in "Road map" on page 10.

About this task

For each of the software installation steps, there are tasks you can perform to verify that the step completed successfully.

The following are some examples of checks you can perform to verify the installation, and the corresponding recovery actions:

Check that the License Compliance Manager administration server has been installed correctly in the Configuration Manager license management extension environment.

Check the system.properties files to verify that the parameter setting **integrationMode**=YES is present in the TLM-CM integration Server settings section of the system.properties file. The system.properties file is located on the administration server in the path <*INSTALL_DIR*>\admin\SLM_Admin_Application.ear\slm_admin.war\WEB-INF\conf on the administration server.

Check the License Compliance Manager fix pack installation trace files. You might have erroneously selected to install just the fixes and not the Configuration Manager license management extension together with the fixes. You can verify the fix pack level installed, as well as whether the Configuration Manager license management extension was selected, by checking the $*INSTALL_DIR*/product.xml file, where, $*INSTALL_DIR* is where the License Compliance Manager infrastructure element is installed. This file is created or updated with the installation of a release or fix pack.

Check that License Compliance Manager agents deployed using the Inventory dependency method have been installed successfully.

From the administration server Web interface, check that the agent is plugged in by selecting **Manage Infrastructure → Agents**.

Verify if the service (tlmagent) on the endpoint is up and running.

Check the Inventory notices group for notices containing installation messages.

Check the installagent return codes. Refer to the *IBM Tivoli License Compliance Manager: Problem Determination* for the installagent return codes.

The endpoint trace file also contains information about the status of the agent deployment. The traces are located in the Tivoli Common Directory in the path COD\logs\install\trace.

Check that agents deployed using the Configuration Manager software package block method have been installed successfully.

There are two ways in which you can verify the success of a software package block installation:

- From the administration server Web interface, check that the agent is plugged in by selecting **Manage Infrastructure → Agents**.
- Verify if the service (tlmagent) on the endpoint is up and running.
- Check the change management status of the software package and the user program exit code in the log file located in the path %BINDIR%/../swdis/work on the Tivoli server.
- Check the endpoint trace file for the status of the agent deployment. The traces are located in the Tivoli Common Directory in the path COD\logs\install\trace on the endpoint.

Check that the Configuration Manager Extension for License Manager is active.

Verify that the Configuration Manager Extension for License Manager is listed among the list of servers on the administration server Web interface by selecting **Manage Infrastructure → Servers**. The default server name is `TMR_Runtime`. If the server name is not listed in the list of servers, perform the following checks:

1. Verify if there are any communication message errors in the tlm_extension<*number*>.log file. See Table 18 on page 90.
2. Verify the name of the server and other parameter in the tlm_extension.ini file. See “The tlm_extension.ini configuration file” on page 83.
3. Check the First-failure data capture trace file. See Table 18 on page 90.

Check that the database federation of the Configuration Manager configuration repository database and the License Compliance Manager administration server database was successful.

Verify that the Apply and Capture services are up and running on the computer where the License Compliance Manager administration server database is installed.

- Windows: use Windows Task Manager to check that the asnapply.exe and asncap.exe processes are active.
- UNIX: run the ps -ef command to check that the asnapply and asncap processes are active.

You can also check the log files for the apply and capture services in the trace file located in the path <*$TLM_INSTALL_DIR*>/admin/db/db2/federation/log on the computer where the administration server database is installed. See “Stopping and starting the replica processes” on page 52 for more information about the replica processes.

Interrupting data flow to the administration server database

For problem determination purposes, you might be required to block the flow of data from the Configuration Manager Extension for License Manager to the administration server database.

You can block data flow from the Configuration Manager Extension for License Manager to the administration server database by stopping the activity on the License Compliance Manager Data Handler. To do this, use the wcollect command to set the –o *max_output_threads* option. Before you change the setting of the *max_output_threads* option, make note of the current setting so that you can reset it to the original value if necessary. Run the command as follows to view the current setting:

```
wcollect @InvDataHandler:tlm_data_handler
```

To set the value to zero run the command as follows:

```
wcollect -o 0 @InvDataHandler:tlm_data_handler
```

This option specifies the maximum number of output threads that the collector can process concurrently. Setting the value to zero halts all activity and files remain in the output queue of the License Compliance Manager Data Handler. After setting the output thread to zero, stop the License Compliance Manager Data Handler using the `wcollect -h immediate` command. To restore the transfer of data to the License Compliance Manager administration server database, reset the output thread to the original value.

Tuning

This section describes how you can change the default configuration of the Configuration Manager license management extension.

You can tune the Configuration Manager license management extension in the following ways:

- “Performance tuning”
- “Configuration files” on page 81
- “Restore the Tivoli objects in the environment” on page 88
- “Environment variables” on page 88

Performance tuning

This section identifies tuning activities to address general and specific performance problems related to the Configuration Manager Extension for License Manager.

For optimal performance of the Configuration Manager Extension for License Manager, consider the following recommendations:

- Choose the appropriate agent deployment method.
- Manage the additional data flow License Compliance Manager brings to the existing Inventory data flow.
- Modify your scan policies and stage your scan schedule to avoid overlap.
- Maintain reasonable values for configuration parameters that are indirectly related.

Agent deployment method

To select the appropriate agent deployment method for your environment, see Chapter 5, “Deploying and configuring agents,” on page 33.

Managing data flow

The Configuration Manager license management extension causes an increased amount of data flowing from the endpoints to the servers. This flow weighs on the Scalable Collector Service (SCS) mechanism to support the combined flow of licensing data and the existing Inventory data.

A solution might be to increase the number of gateways to support an increased SCS load, however, this solution is not acceptable or even feasible in most environments.

To balance the load on all components in the infrastructure, you can change the default value of the -b *checkpoint_mode* parameter to control the input and output queues of the gateway collectors. Remember to stop the gateway collector before changing this parameter. This parameter is set using the wcollect command. The default value of the parameter is `full`. This means that the entire queue is dumped to the file system when a new checkpoint is requested. In the Configuration Manager license management extension, set the value to `incremental` so that only the differences are written to the file system instead of the entire queue, when a checkpoint is requested. This setting optimizes queue handling optimization and improves gateway response.

Note: Although only the differences in the queue are written to the file system with *checkpoint_mode*=`incremental`, a full dump of the queue occurs at time intervals defined by the -a *full_dump_queue_time*. The collector needs to do a full dump of the queues in order to compact the incremental changes stored to the file system and to reduce the disk space used.

Changing the Configuration Manager scan policy

Peak data flow periods are usually triggered by scan activities. To minimize peak effects in the Configuration Manager license management extension environment, you can adopt the following policies:

- Adopt the License Compliance Manager scheduled scan and use it exclusively. A License Compliance Manager scan triggers a Configuration Manager Inventory scan to maintain database synchronization. It is not necessary to invoke scans from both products.
- Since License Compliance Manager scans are scheduled by division, it is important to define a staged scan schedule for each division to avoid overlap and data flow overload.
- Scheduling scans by division, emphasizes the importance in planning and defining agent - division associations carefully.

Relationships between configuration parameters

Baseline data flow of the Configuration Manager license management extension is comprised of a number of files that are produced by the agent and uploaded to the License Compliance Manager administration server. The following types of files are produced:

- .lic files: usage data, inventory scan data, and agent machine topology

- .unk files: potential signatures
- .plg files: plugin data

The frequency with which these files are uploaded are managed by three integrated agent configuration settings defined in the agents_config.ini configuration file. These settings are configurable and are directly related to some of the License Compliance Manager administration server configuration settings defined in the system.properties file. Table 9 shows which configuration settings are related.

Table 9. Relationship between configuration parameters

agents_config.ini	**Description**	**system.properties**
offlineUsagePeriod	When there is use or inventory data, the agent sends a (.lic) file with the frequency defined by the offlineUsagePeriod.	aggregateUsagePeriod maxAggregateUsageAge productInventoryBuilderPeriod
pingPeriod	Defines the frequency with which a heartbeat notification is sent. (.plg)	maxAgentInactivity
uploadMinTime	If the potential (unknown) signature files upload mechanism is enabled, this period defines the frequency with which potential signatures are sent (.unk).	

Changes to these parameter settings imply that the License Compliance Manager administration server configuration settings must be updated accordingly to maintain coherency between the settings. For example, the pingPeriod value can be significantly extended if the maxAgentInactivity value is high. The value of pingPeriod must always be inferior to the maxAgentInactivity value to avoid agents that are active be reported as inactive on the License Compliance Manager administration server Web interface.

Configuration files

This section describes the configuration files for the Configuration Manager license management extension.

Configuration Manager license management extension maintains the following configuration files that you can use to tune the extension to suit your needs:

- Configuration Manager configuration files. Refer to *Configuration Manager: User's Guide for Software Distribution*, and *Configuration Manager: User's Guide for Deployment Services*.
- Configuration Manager license management extension configuration files. See "Configuration Manager license management extension configuration files."
- License Compliance Manager configuration files. See "License Compliance Manager configuration files" on page 82.

Configuration Manager license management extension configuration files

Table 10 on page 82 provides a summary of the Configuration Manager license management extension configuration files that you can edit.

Table 10. Configuration Manager license management extension configuration files

Configuration file	Usage
tlm_extension.ini	Defines the configuration parameters of the Configuration Manager Extension for License Manager component. See "The tlm_extension.ini configuration file" on page 83.
wcmeupld.ini	Defines the configuration parameters of the Configuration Manager Endpoint Extension component. See "The wcmeupld.ini configuration file" on page 85.
agents_config.ini	Defines agent configuration parameters. See "The agents_config.ini configuration file" on page 86.

License Compliance Manager configuration files

Table 11 provides a summary of the License Compliance Manager configuration files that you can edit.

Table 11. License Compliance Manager configuration files

Configuration file	Usage
system.properties	The main configuration file of the administration server. It defines the administration server configuration and e-mail configuration settings. Refer to *IBM Tivoli License Compliance Manager: Planning, Installation, and Configuration* for information about the configuration settings in this file. Some new parameters have been added to this file for the Configuration Manager license management extension. See "The system.properties configuration file" on page 87.
log.properties	Defines the trace parameters for the administration server. See the *IBM Tivoli License Compliance Manager: Problem Determination* for full details. These are the only parameters that can be changed and reloaded while a server is running. See the logreload command, described in *IBM Tivoli License Compliance Manager: Problem Determination*.
tlmagent.ini	Defines the configurable values of the trace component for the agent. It contains settings for trace level, trace file sizes, and number of trace files.

Refer to *IBM Tivoli License Compliance Manager: Problem Determination* and *IBM Tivoli License Compliance Manager: Planning, Installation, and Configuration* for more information about these and other configuration files.

The tlm_extension.ini configuration file

This section describes the configuration parameters of the Configuration Manager Extension for License Manager component.

After the installation of the Configuration Manager Extension for License Manager, a file named tlm_extension.ini is created in the path *$DBDIR*/tlm_handler.

The tlm_extension.ini file contains the following information:

- "Configuration Manager Extension for License Manager parameters."
- "Administration server communication parameters" on page 84.

Configuration Manager Extension for License Manager parameters

Table 12 shows the parameters defined in the tlm_extension.ini file that you might need to change. You should not change any other setting in this configuration file. If you specify a value for a parameter that is out of range, or if no value is specified, then the default value is used.

Table 12. Configuration parameters of the Configuration Manager Extension for License Manager component

Parameter	Units	Default	Minimum	Maximum
	Description			
wake_up_frequency	seconds	60	15	300
	Specifies the wake-up interval between the processing of new data uploaded from the agents.			
shutdown_timeout	minutes	30	5	10080
	Specifies the timeout, in minutes, after which the server shuts down when idle. If the specified value is out of range or if no value is specified, then the default value is used.			
trace_level	integer	0	0	3
	Specifies the trace level. Valid levels are: [0, 1, 2, 3]. **0** Traces are disabled. **1** Reports only errors. **2** Reports errors and warnings. **3** Reports errors, warnings, and informational messages. Any value greater than 3 produces the same effect as 3. Any value lower than 0 produces the same effect as 0.			
traces_files_num	number of files	3	1	1000
	Specifies the number of trace files generated. If the specified value is out of range or if no value is specified, then the default value is used.			
trace_max_size	bytes	1000000	1	2000000000
	Specifies the maximum size of each trace file generated. If the specified value is out of range or if no value is specified, then the default value is used.			

Table 12. Configuration parameters of the Configuration Manager Extension for License Manager component (continued)

Parameter	Units	Default	Minimum	Maximum
	Description			
log_level	integer	3	0	3
	Specifies the log level. Valid levels are: [0, 1, 2, 3]. **0** Logs are disabled. **1** Reports only errors. **2** Reports errors and warnings. **3** Reports errors, warnings and informational messages. Any value greater than 3 produces the same effect as 3. Any value lower than 0 produces the same effect as 0.			
log_max_size	bytes	1000000	1	2000000000
	Specifies the maximum size of each log file generated. If the specified value is out of range or if no value is specified, the default value is used.			
max_pkg_file_size	bytes	200000	1	400000
	Specifies the maximum size of a single packet of data sent to the administration server when agent information collected from the agent is uploaded. When the addition of a new file would cause the packet to exceed the maximum size, the Configuration Manager Extension for License Manager starts a new packet. **Note:** If the size of a single file received from the agent exceeds the size of the value set for this parameter, this file is contained in a single packet, even though it exceeds the configured maximum size.			
max_logic_error_retry_count	integer	3	1	1000
	Specifies the maximum number of times the Configuration Manager Extension for License Manager attempts to send a package to the administration server unsuccessfully, with a logic error return code, before giving up and discarding the package.			
depot_size	Megabytes	10000	4	10000
	Specifies the maximum size of the depot directory. This is the directory information received from the agent that is stored before being uploaded to the administration server. If the configured size is exceeded, the oldest files are deleted until the size is reduced to three-quarters of the configured maximum. The default value, which is also the maximum value, is considered to be a value that will not be exceeded during normal operation. For this reason the check on the maximum size is not performed and there is no risk that files will be deleted. If you decide to reduce the maximum depot size, be aware that you could risk losing data that has not yet been transmitted to the administration server.			

Administration server communication parameters

Table 13 on page 85 describes the Tivoli License Manager Administration Server communication parameters defined in the tlm_extension.ini file.

Table 13. License Compliance Manager administration server communication parameters

Parameter	Description
tlm_server_name	License Compliance Manager administration server address (IP address or hostname).
tlm_server_port=80	License Compliance Manager administration server HTTP port.
tlm_server_uri=/slmadmin/service	License Compliance Manager administration server servlet path.
tlm_customer_name=IBM_CM	Organization name. This is the name specified during the installation of the License Compliance Manager administration server database infrastructure element.
tlm_runtime_name=TMRtest	Name of the Configuration Manager Extension for License Manager. This name corresponds to the value you specified when you installed the Configuration Manager Extension for License Manager. Ensure that this name also matches the License Manager Extension name you specify when installing License Compliance Manager on the administration server database.

If you encounter communication problems between the Configuration Manager Extension for License Manager component and the License Compliance Manager administration server, verify the values of the administration server communication parameters.

The wcmeupld.ini configuration file

This section describes the configuration parameters of the Configuration Manager Endpoint Extension component that uploads agent data to the administration server database.

The wcmeupld.ini configuration file is created the first time the Configuration Manager Endpoint Extension component runs and is created in the path *%LCF_ROOT%*\cme. You can use this file to modify the behavior of the Configuration Manager Endpoint Extension component. Table 14 shows the parameters defined in the wcmeupld.ini file.

Table 14. Configuration parameters of the Configuration Manager Endpoint Extension component

Parameter	Units	Default	Minimum	Maximum
	Description			
trace_size	bytes	10000000 (10 MB)	1000000	no limit
	Defines the maximum size of a single iteration of the wcmeupld<*number*>.trc trace file. When the maximum size is reached, the file is renamed and new trace file is started.			
trace_level	integer	0	0	6
	Defines the level of trace to be logged. The default level, 0, means no traces enabled.			
min_queue_disk_space	megabytes	30	10	no limit
	The minimum space required for the queue of the Configuration Manager Endpoint Extension before it is declared full (on OS/400, the default value is 10 MB).			

Table 14. Configuration parameters of the Configuration Manager Endpoint Extension component (continued)

Parameter	Units	Default	Minimum	Maximum
	Description			
max_queue_num_dir	integer	8	3	no limit
	The data uploaded from the endpoint to the administration server is stored in a number of directories on the endpoint. This parameter determines the maximum number of directories permitted in the queue before it is declared full.			
upcall_completion_timeout	seconds	300	30	no limit
	The amount of time the upcall manager waits for an indication from mcollect about how the upcall went. If, within this period, the upcall manager receives notice that mcollect completed the upcall successfully, then the data on the endpoint is deleted. If no notice is received from mcollect, the upload of data is retried.			

The agents_config.ini configuration file

This section describes the configuration parameters of the Configuration Manager license management extension agent.

The first time the Configuration Manager Extension for License Manager starts, a file named agents_config.ini is created in the path *$DBDIR*/tlm_handler/agent_data. This file contains the configuration parameters that can be sent to the agents using the **wtlminfoget** command.

Table 15 shows parameters defined in the agents_config.ini file that you might need to change. You should not change any other setting in this configuration file.

Table 15. Configuration Manager license management extension agent

Parameter	Units	Default	Minimum	Maximum
	Description			
pingPeriod	minutes	4320 (3 days)	60	10080
	The length of time the agent waits to send a package confirming the agent is up and running.			
offlineUsagePeriod	minutes	720 (12 hours)	30	10080
	The time interval between uploads of any offline use data to the server.			
processListPeriod	seconds	360	60	600
	The interval between compilation of consecutive versions of the agent process list. Comparison of consecutive versions of the agent process list enables the agent to determine which applications have started or stopped in the intervening time. If the period is too long, applications might start and stop during the interval and so not be included in the software use information collected by the agent.			
sysConfUpdatePeriod	minutes	80	30	10080
	The interval at which the agent performs updates of hardware information about the node or partition where it is running.			
wasAgentCheckPeriod	minutes	120 (2 hours)	10	10080
	The interval at which the agent checks to ensure that the WebSphere Application Server agent is running.			

Table 15. Configuration Manager license management extension agent (continued)

Parameter	Units	Default	Minimum	Maximum
	Description			
uploadMinTime	minutes	1440	100	10080
	If the upload mechanism is enabled, the time interval between uploads of potential file information to the server.			

The system.properties configuration file

This section describes the new configuration parameters of the system.properties file on the administration server.

The system.properties file is the main configuration file of the License Compliance Manager server. The parameters of the file are fully described in *IBM Tivoli License Compliance Manager: Planning, Installation, and Configuration*.

Some new parameters are introduced for the Configuration Manager license management extension.

Table 16 shows the new parameters defined in the system.properties file that you might need to change.

Table 16. Configuration parameters of the system.properties file on the administration server

Parameter	Units	Default	Minimum	Maximum
	Description			
integrationMode	Boolean	true	false	true
	Indicates if License Compliance Manager is enabled to communicate with the Tivoli management region server. Valid values are [true, false]. **True** Configuration Manager license management extension **False** Classic License Compliance Manager			
maxAgentInactivity	minutes	10 080	1 440	129 600
	The maximum time interval before a Configuration Manager license management extension agent is considered inactive. The inactive state can be verified on the License Compliance Manager administration server Web interface selecting **Manage Infrastructure** → **Agents**.			
catalogBuilderPeriod	minutes	1 440	60	10 080
	The period of time between consecutive builds of the catalog by the administration server if it has been changed.			
storeUser	boolean	true	false	true
	Indicates whether information about the user is to be included in use data. Possible values are: **true** User information is included. **false** User information is not included.			

Restore the Tivoli objects in the environment

This section describes how you restore the Tivoli objects created in your environment by the installation of the Configuration Manager Extension for License Manager component.

Before you begin

If the Tivoli objects created by the installation are accidentally deleted from your environment or, if for any reason you need to restore this environment, you can rebuild it by manually running a script. See “Objects created by the installation” on page 21 for information about what is created in your environment.

About this task

To rebuild the environment originally created by the installation, do the following:

1. Locate the script in the following path: $BINDIR/TME/TLM_EXT/SCRIPTS/ on the computer where you installed the Configuration Manager Extension for License Manager component.
2. Run the TLM_EXT_build_env.sh script as follows:

   ```
   TLM_EXT_build_env.sh -a [log_path]
   ```

   where *log_path* indicates the path to the log file that is generated by the script. If you do not specify the *log_path*, then, by default, a log file named, tlm_ext_build_env.log, is created in the directory where Tivoli products create temporary files. You can verify this directory by running the **wtemp** command. Refer to the *Tivoli Management Framework Reference Manual* for details about this command.

What to do next

The script recreates all the required objects and resets all the scheduling parameters. See “Objects created by the installation” on page 21 for a list of the required objects created.

Note: If you made any changes to tasks or jobs after the installation, these changes are lost after running the TLM_EXT_build_env.sh script.

Environment variables

This section describes some of the environment variables to change the behavior of the Configuration Manager Extension for License Manager.

The following environment variables can be set to change the behavior of the Configuration Manager Extension for License Manager:

Table 17. Environment variables

Environment variable	Description
TLM_HANDLER_DEBUG	When defined in the environment, it enables the generation of additional traces for component. The traces are stored in the path, $DBDIR/tlm_handler/log/ tlm_ext_core.trc and are created at the start up of the component.

Table 17. Environment variables (continued)

Environment variable	Description
TLM_HANDLER_PORT	Specifies the TCP/IP port to be used by the Java server to communicate with the CORBA object. If it is not specified, the default port used is 10000.
TLM_HANDLER_JVM_OPTS	Specifies optional parameters that are passed to the Java process. If not specified, the default parameter **-Xmx256m** is used. A typical use of this variable is to increase the maximum heap size of the Java Virtual Machine if the default value is not sufficient. Multiple options can be specified by separating them with the comma (,) character.
TLM_HANDLER_LOCALHOST	Specifies the IP address used by the CORBA object to contact the Java process. By default, the value 127.0.0.1 is used. You might need to set this variable on multihomed machines if the Configuration Manager license management extension component is not automatically able to detect the correct IP address. A multihomed machine is a computer host that has multiple IP addresses to connected networks.

Verifying environment variables

Tivoli environment variables are set using the Tivoli command odadmin environ set. On managed nodes, you can verify these settings by entering the following command:

```
odadmin environ get
```

Setting environment variables

To modify the value of an environment variable, you must first invoke the `odadmin environ get` command, then modify the file containing the variable, then invoke the odadmin environ set command, specifying the file containing the variable as follows:

```
odadmin environ set > filename
```

For additional information about the **odadmin environ** command, refer to the *Tivoli Management Framework Reference Manual*.

Traces and logs

This section describes the traces and logs available to help you in problem determination.

The following topics describe the problem determination support available to resolve problems that can occur when installing or using the product.

- “Configuration Manager license management extension trace and log files” on page 90
- “License Compliance Manager trace and log files” on page 92

Configuration Manager license management extension trace and log files

This section describes the trace and logs available with of the Configuration Manager license management extension.

There are traces and logs available for both server and endpoint components.

The Configuration Manager Extension for License Manager trace settings are defined in the tlm_extension.ini configuration file on the Tivoli management region server computer. When enabled, trace files are stored in the following directory: $DBDIR/tlm_handler/log on the nodes where the Configuration Manager Extension for License Manager component is installed.

Configuration Manager Endpoint Extension trace settings are defined in the wcmeupld.ini file.

The **wcollect** command is used to enable the traces of License Compliance Manager Data Handler. Refer to *IBM Tivoli Configuration Manager: User's Guide for Inventory* for more information about the **wcollect** command.

Table 18 lists the Configuration Manager Extension for License Manager traces and logs.

Table 18. Configuration Manager Extension for License Manager traces and logs

Trace or log file	Description	Path
TLMHandler.trc	When the Configuration Manager Extension for License Manager server starts, there is an initial phase when the tracing is not yet initialized. If a problem occurs during this initial phase, it cannot be traced. The TLMHandler.trc trace file has been created to address this timeframe during which regular tracing is not available.	$HOME directory of the user under which the java process runs. You define and modify this user using the **widmap** command. Refer to the *Tivoli Management Framework Reference Manual* for information about this command.
ffdc.trc	A file that logs all activities performed by the Configuration Manager Extension for License Manager component in case of failure or unexpected behavior. This function is always enabled even if traces are disabled.	$DBDIR\tlm_handler\log

Table 18. Configuration Manager Extension for License Manager traces and logs (continued)

Trace or log file	Description	Path
ITLMInfo.1.log	This log reports the change management status of the distribution of the ITLMInfo.1 software package submitted by the **wtlminfoget** command, as well as the return codes of the execute user programs defined in the software package. See "Return codes for ITLMInfo.1 software package" on page 92.	$BINDIR\..\swdis\work
tlm_extension.<*number*>trc	The trace file for the Configuration Manager Extension for License Manager component.	$DBDIR\tlm_handler\log
tlm_extension<*number*>.log	This file logs all activities performed by the Configuration Manager Extension for License Manager.	$DBDIR\tlm_handler\log
mcollect.log	The log of the License Compliance Manager Data Handler.	$DBDIR\tlm_data_handler\ mcollect.log

Table 19 lists the traces and logs for the Configuration Manager Endpoint Extension.

Table 19. Configuration Manager Endpoint Extension traces and logs

Trace or log file	Description	Path
wcmeupld<*number*>.trc	Traces the Configuration Manager Endpoint Extension component and is located on the endpoint. When this file reaches its maximum size, it is renamed wcmeupld1.trc, and a new trace file is started. If wcmeupld1.trc, already exists, it is renamed wcmeupld2.trc, and so on. When the maximum number of files is reached, wcmeupld9.trc, the process starts over again.	$LCF_DATDIR\..\..\cme\ trace
cmefile.log	A log file is created each time a software package is distributed. Located on the endpoint, this file logs the outcome of the distribution of the ITLMInfo1.sp using the **wtlminfoget** command.	$LCF_DATDIR\..\..\cme\ dat

Return codes for ITLMInfo.1 software package

The distribution of the ITLMInfo.1 package submitted by the **wtlminfoget** command at the endpoint might fail for several reasons. The Software Distribution log file, ITLMInfo.1.log, associated to the ITLMInfo.1 package reports the return code of the operation.Table 20 lists the possible error codes that can be logged:

Table 20. Return codes logged to the Software Distribution log file

Return Code	**Description**
0	Operation successful.
10	The command was invoked with an incorrect number of parameters.
11	The requested operation is not valid.
12	The License Compliance Manager agent is not installed.
13	The **tlmagent** -*impcat* command failed.
14	The **tlmagent** –*parameter* command failed
15	Both `tlmagent –impcat` and `tlmagent` –*param* commands failed.
16	License Compliance Manager agent is stopped.
17	The agent is busy.

License Compliance Manager trace and log files

This section describes License Compliance Manager traces and logs.

Trace levels, trace files, log files and their locations are fully described in *IBM Tivoli License Compliance Manager: Problem Determination* for the following License Compliance Manager infrastructure elements:

- Agent and WebSphere Application Server agent
- Administration server
- Catalog manager
- Command line

The following License Compliance Manager trace and log files are related to the Configuration Manager license management extension.

Database federation trace and log files

Table 21 lists the trace and log files related to the database replication services, Apply and Capture.

Table 21. Database federation trace and log files

Trace or Log file	**Description**	**Path**
Apply: <*db_instance_name*>.TLMA. TCM_CAT_A.APP.log **Capture**: <*db_instance_name*>.TLMA. ASN.CAP.log	The log files of the Apply and Capture replica services that are started automatically on the administration server database computer after the installation.	<INSTALL_DIR>/admin/db/db2/federation/log
TCM_CAT_A.trc	This trace file is created when the replica services start and gets written to if the apply service encounters an exception	<INSTALL_DIR>/admin/db/db2/federation/log

Diagnosing problems

This section provides information to help you diagnose problems with the license management extension in your Configuration Manager environment.

Diagnosis information such as, common symptoms and their cause and solution, is divided into the following categories:

- Installation
- Databases
- Servers
- Agent operation
- Communication
- Installed software reports
- Software use reports

Refer to *IBM Tivoli License Compliance Manager: Problem Determination* for more problem diagnosis information related to License Compliance Manager infrastructure elements.

Installation

Symptom: Problem with Configuration Manager configuration repository database connection.

Causes and solution:
Depending on the vendor of the Configuration Manager configuration repository database, there are different checks you can perform to solve the problem.

Table 22. Checks to verify the database connection

Location	Oracle database	DB2 database
Local	Verify that the database is accessible with the service name and credentials provided.	Verify that the database is accessible using the TLMIDB alias and the credentials provided during installation.
Remote	Verify that the Oracle client is installed on the local machine, and that the Configuration Manager configuration repository database is accessible from the local machine with the service name and credentials provided during installation.	Verify that locally the TCMNODE has been cataloged correctly, and that the remote Configuration Manager configuration repository database is accessible using the TLMIDB alias and the credentials provided during installation.

Symptom: An error occurs during the database federation when the Configuration Manager configuration repository database is an Oracle database.
Problem during the installation of the License Compliance Manager administration server database, at the Performing Database Federation step, and when the Configuration Manager configuration repository database is an Oracle database.

Causes and solution:
Verify that the WebSphere Information Integrator has been installed

correctly on the computer where the License Compliance Manager administration server database is installed. If you must run the step Performing Database Federation a second time after a failure, run the following script first: *<INSTALL_DIR>*/admin/db/db2/federation/dbrootlauncher.bat/sh uninstallfed.bat/sh.

Symptom: Error verifying information for the Configuration Manager configuration repository database.

Error verifying information for the Configuration Manager configuration repository database when installing License Compliance Manager administration server database. The administration database is installed on same machine as the Configuration Manager configuration repository database and the Configuration Manager configuration repository database is not installed in /home/<*instance_owner*> and so the database is not accessible using the alias TLMIDB created during the installation.

Causes and solution:

Install the administration server database on a computer different from the Configuration Manager configuration repository database.

Symptom: Deployed agents not displaying on the administration server Web interface.

Agents deployed using the Configuration Manager software package block method or the inventory dependency method are not visible from the License Compliance Manager administration server Web interface.

Causes and solution:

If the deployed agents are not listed when you select **Manage Infrastructure** → **Agents** from the Web interface then perform the following checks:

1. If you deployed the agent using the inventory dependency method, check the Inventory notices group for notices containing installation error messages.

   If you deployed the agent using the software package block method, check the change management status of the distributed software package and the user program exit code in the log file located in the path $BINDIR/../swdis/work on the Tivoli server.
2. If error messages are reported, check the agent trace file containing information about the status of the agent deployment. The agent installation trace file is located in the Tivoli Common Directory in the path COD/logs/install/trace.
3. If no error messages are reported, and you have enabled the traces for the agents, the Configuration Manager Endpoint Extension, the License Compliance Manager Data Handler, the License Compliance Manager handler, and the gateway collector, then you can track the successful transfer of a plugin file, .plg, that is produced by the agent in the path $LCF_DATDIR/../../inv/TLM_TMP. The plugin file is transferred to the administration server through the Configuration Manager license management extension infrastructure. See “Configuration Manager license management extension trace and log files” on page 90 for information about the trace and log files available.

Symptom: Updated information is missing from the software use and inventory reports on the administration server. database.

Causes and solution:

If you have uninstalled and then reinstalled the Inventory server component, you must also recreate the License Compliance Manager Data Handler by running the **wtlmdh** command. See "wtlmdh" on page 71 for the command syntax and usage.

Symptom: License management extension agent uninstalled successfully, but an error message is displayed indicating that the uninstallation was not successful.

Causes and solution:

The following error message is displayed even though the agent is successfully uninstalled:

```
 CPF35D2 PTF 1IBMTLM-22F0001 not removed. The following warnings
were generated: Could not delete the product uninstaller resources.
```

To verify that the uninstallation procedure was successful, access the PTF panel on the OS/400 console and check that the PTF for the product 1IBMTLM is not present then, run the `go licpmg` command and check that the agent is no longer present.

Symptom: Updated information is missing from the software use and inventory reports on the administration server. database.

Causes and solution:

If you have uninstalled and then reinstalled the Inventory server component, you must also recreate the License Compliance Manager Data Handler by running the **wtlmdh** command. See "wtlmdh" on page 71 for the command syntax and usage.

Databases

Symptom: Data is not being synchronized in the Configuration Manager configuration repository database.

Operations which modify the catalog tables of the administration server database are not triggering a replica process to synchronize the same information in the Configuration Manager configuration repository database as they should. Examples of such operations are importing the catalog, a subsequent update to a full catalog, registering a potential signature using Catalog Manager, and enabling and disabling products for monitoring.

Causes and solution:

Verify that the apply and capture replica services are up and running. Check the apply service trace file and perform problem determination based on the contents of the file. See Table 21 on page 92. The frequency with which table views are duplicated in both the Configuration Manager configuration repository database and the administration server database is set by default to 20 minutes. Adjust the frequency for a shorter time period. You can configure this frequency as follows: **Control Centre** → **Replication Centre** → **SQL Replication** → **Definition** → **APPLY Control Servers** → **TLMA** → **Subscription Sets** . Modify the Subscription Set properties.

Servers

Symptom: Problems running tasks from *License_Management-<TMR_region_name>* **policy region and running wtlminfoget command.**

If you fail to perform tasks from the *License_Management-*

<*TMR_region_name*> policy region successfully or have problems running the **wtlminfoget** command, the environment automatically created on the Tivoli desktop by the installation might be corrupt or might have been erroneously removed.

Causes and solution:

Rebuild the environment by running the TLM_EXT_build_env.sh script. See“Restore the Tivoli objects in the environment” on page 88 for details.

Symptom: The Tivoli management region server (Tivoli server) appears to be inactive from the administration server Web user interface.

The administration server cannot communicate with the Tivoli server. The Tivoli server, registered as a runtime server, appears to be inactive from the administration server Web user interface.

Causes and solution:

Verify that the parameters specified during the installation of the Configuration Manager Extension for License Manager component and the parameters in the tlm_extension.ini file are aligned.

Symptom: The Tivoli server returns an error code in attempting to register with the administration server.

The Tivoli server returns an error code in attempting to register with the administration server, even if the administration server Web user interface displays the Tivoli server as active.

Causes and solution:

If you are using WebSphere Application Server version 6.0.2.9, then the Administration server Web user interface displays the Tivoli management region server as plugged in and active, however, the Configuration Manager Extension for License Manager log file reports that the extension component is not able to register with the License Compliance Manager administration server. Also, you are not able to view agents connected to the server from the administration server Web user interface

Apply the following fix to solve this problem: APAR PK23493. Before applying the fix, verify this problem by changing the port number in the tlm_extension.ini file to the port number of the WebSphere Application Server instead of the HTTP server. If the communication problems resolve, then proceed to apply the fix.

Agent operation

Symptom: Submitting the wtlminfoget command with the -c DELTA option specified fails and return code error 13 is reported.

Causes and solution:

The **wtlminfoget** command with the **-c DELTA** option specified failed because a previous impcat operation failed on one or more endpoints. The impcat command might have failed because the agent was stopped or busy.

Submit the command again specifying the **-c FULL** option on those endpoints where the **-c DELTA** submission failed with return code 13. If the **-c FULL** submission is successful, then any future **-c DELTA** submissions will succeed.

Communication

Symptom: Communication problems between the License Compliance Manager administration server and the Configuration Manager Extension for License Manager

Following the installation or, even after the product integration is up and running, the Configuration Manager Extension for License Manager does not display as **Active** among the list of servers when you select **Manage Infrastructure** → **Servers** from the portfolio of the License Compliance Manager administration server Web interface.

Causes and solution:

There are several check you can perform to verify the communication problem:

- Verify that the value of the parameter **integrationMode** is set to `true` in the system.properties file on the administration server. The parameter is defined in the TLM-CM integration Server settings section of the system.properties file. See "The system.properties configuration file" on page 87.
- Verify whether there are inconsistencies between the License Manager Extension Name provided during the installation of the Configuration Manager Extension for License Manager and the name provided during installation of License Compliance Manager. Check that the value of the **tlm_runtime_name** parameter, defined in the administration server communication parameters, of the tlm_extension.ini file corresponds to the name that displays on the administration server Web interface when you select **Manage Infrastructure** → **Servers** from the portfolio. If the value of this parameter is changed, it must also be changed from the administration server Web interface. If the name is changed on the Web interface, the value of the **tlm_runtime_name** parameter must also be changed. See "Administration server communication parameters" on page 84.
- Verify that the IBM HTTP Server is up and running on the computer where the administration server is installed.
- Check for details about the problem by consulting the License Compliance Manager handler first-failure data capture trace file, ffdc.trc stored in the path $DBDIR/tlm_handler/log.

Installed software report

Symptom: Following the deployment of an agent, a software scan that is registered on the administration server produces an empty installs snapshot or does not include a product you know is installed.
Symptom: Following a new product installation on an agent, a software scan that is registered on the administration server produces an empty installs snapshot.

Causes and solution:

There are several checks you can perform to trace the flow of data to determine at which point the process failed.

1. Verify that the scan was performed on the agents. From the License Compliance Manager administration server Web interface, use the **Manage Infrastructure** → **Agents** task from the portfolio to check the agent details for an individual agent.

The agent details contain information about the last scan time. The last scan time is the last time a scan was performed on the agent.

2. If a last scan time exists, verify that the scan data collected on the agent has been processed by the License Compliance Manager administration server. The administration server configuration includes the **productInventoryBuilderPeriod** parameter defined in the system.properties configuration file. This parameter controls the frequency with which the administration server rebuilds the inventory using the installed software information collected by the agents. Until the inventory build process is completed, the scan information is not available in the installed software report. To verify if the task ran, check the value of the LAST_INVENTORY_EXEC_TIME field in the ADM.CONTROL table in the administration server database. A value assigned to the LAST_INVENTORY_EXEC_TIME field indicates that this internal task has run and the last time it was run.
3. If the internal task regulated by the productInventoryBuilderPeriod parameter has run, then perform the following checks on the endpoint:
   a. Verify that a valid software catalog is present in the agent cache by submitting the command `tlmagent -expcat` on the agent. Compare the timestamp defined in the exported catalog with the timestamp in the catalog created by the administration server in the path <*TLM_INSTALL_DIR*>/admin/SLM_Admin_Application.ear/slm_admin.war/agent. The timestamp defined in the catalog created by the administration server is based on the value of the **ADM_CAT_SEQUENCE_TIME** field in the SWCAT.CONTROL table.
   b. If the software catalog in the agent cache is valid, then verify that the file, matched_signatures.xml, exists in the path $LCF_DATDIR/../../itlm/scanner with a timestamp valid for the scan time. This file is produced by the agent when it performs the software scan. If this file is empty, check the agent log files to determine the problem.
   c. If the matched_signatures.xml file exists and is valid, and you have enabled the traces for the agents, the Configuration Manager Endpoint Extension, the License Compliance Manager Data Handler, the License Compliance Manager handler, and the gateway collector, then you can track the successful transfer of the .lic file that is produced by the agent in the path $LCF_DATDIR/../../inv/TLM_TMP. The .lic file is transferred to the administration server through the Configuration Manager license management extension infrastructure. See “Configuration Manager license management extension trace and log files” on page 90 for information about the trace and log files available.

Software use report

Symptom: An empty software use report is produced.

Products that you know have been in use on monitored agents do not appear in the software use reports.

Causes and solution:

There are several checks you can perform to determine possible causes for this:

1. Verify that products enabled for monitoring are found on the monitored agents.
   a. Ensure that a successful software scan has been performed and processed by the administration server. To do this, from the License Compliance Manager administration server Web interface, produce an Installs Snapshot using the **Produce Reports** → **Installs Snapshot** task from the portfolio.
   b. Verify that the products you are expecting to see in the use report are enabled for monitoring. By default, use monitoring of products is disabled. You can enable monitoring by creating a license or by changing the monitoring property of the product using the **Define Product Properties** → **Define Monitoring** task from the License Compliance Manager administration server Web interface portfolio.
2. If the products are reported to be installed by the Installs Snapshot report, then verify that the use data has been aggregated by the License Compliance Manager administration server. This internal task is regulated by two parameters defined in the system.properties configuration file on the administration server, **aggregateUsagePeriod** and **maxAggregateUsageAge**. The **aggregateUsagePeriod** defines how often the aggregation process runs and the **maxAggregateUsageAge** defines how old the use data must be before it is aggregated. This setting is used to ensure that all the relevant data for an aggregation has arrived at the administration server before the aggregation of use data. Refer to IBM Tivoli License Compliance Manager: Planning, Installation, and Configuration for information about these parameters.

   You can also verify that the usage data has been aggregated by checking the value of the FIRST_TO_AGGREGATE_DAY field in the ADM.CONTROL table of the administration server database.
3. If the value of the FIRST_TO_AGGREGATE_DAY field confirms that the internal task has run, then perform the following checks on the endpoint:
   a. Verify that a valid software catalog is present in the agent cache by submitting the command `tlmagent -expcat` on the agent. In the exported catalog produced by this command, check that the components associated to the products enabled for monitoring are enabled in the software catalog. If a valid software catalog is not found, download the latest software catalog from the administration server to the agent by running the **wtlminfoget** command.

b. If the software catalog present in the agent cache is valid, check that the value of the **processListPeriod** parameter is reasonably low. This parameter is defined in the agents_config.ini configuration file on the Tivoli server or on the computer where the Configuration Manager Extension for License Manager is installed. Comparison of consecutive versions of the agent process list enables the agent to determine which applications have started or stopped in the intervening time. If the period is too long, applications might start and stop during the interval and so not be included in the software use information collected by the agent.

c. If usage data is discovered, and you have enabled the traces for the agents, the Configuration Manager Endpoint Extension, the License Compliance Manager Data Handler, the License Compliance Manager handler, and the gateway collector, then you can track the successful transfer of the .lic file that is produced by the agent in the path $LCF_DATDIR/../../inv/TLM_TMP. The .lic file is transferred to the administration server through the Configuration Manager license management extension infrastructure. See “Configuration Manager license management extension trace and log files” on page 90 for information about the trace and log files available.

Chapter 13. Uninstalling the license management extension

This chapter describes how you uninstall the license management extension from your Configuration Manager environment.

Removing the extension from License Compliance Manager

The following are the tasks to remove the Configuration Manager license management extension from the License Compliance Manager infrastructure.

1. Unfederate the databases. The database federation involves a set of components installed on the License Compliance Manager administration server database. Before removing the federation, ensure that the replica process are not running. See "Stopping and starting the replica processes" on page 52. You remove the federation from the administration server database by running the following script. The user must be the License Compliance Manager administration server DB2 database instance owner to run the script.

   Windows
   uninstallfed.bat

   UNIX uninstallfed.sh

   After running the script, the software catalog is no longer copied from the administration server database to the Configuration Manager configuration repository database.

   Note: If you were required to install the WebSphere Information Integrator, this script does not remove it.
2. Disable the Configuration Manager license management extension on the administration server. Change the value of the **integrationMode** parameter in the system.properties file to `False`.

Removing License Compliance Manager from the Configuration Manager environment

To remove the license management capabilities from your Configuration Manager environment, perform the following tasks:

1. Stop and disable the License Compliance Manager agent on the endpoint by distributing the stopITLMAgent software package to it. See "Enabling and disabling agents using software packages" on page 48. This step is performed to prevent the upload of data from the agent.
2. Stop the Configuration Manager Extension for License Manager component using the **wtlmhandler** command. See "wtlmhandler" on page 73 for the command syntax and usage.
3. Uninstall the Configuration Manager Extension for License Manager component. As a result, the Inventory component of Configuration Manager assumes its traditional role in the environment. Specifically, the Inventory Data Handler discards all files containing License Compliance Manager information. See "Uninstalling the license management extension components" on page 103.
4. Delete the License Compliance Manager tables from the Configuration Manager configuration repository database. On the computer where the Configuration Manager configuration repository database is installed, run the appropriate

script to remove the database federation. You must be the Configuration Manager configuration repository database instance owner to run the script.

- inv_undo_db2_fed_schema.sql
- inv_undo_ora_fed_schema.sql

The script files are located in the path $BINDIR/TME/TLM_EXT/SCRIPTS on the computer where the Configuration Manager Extension for License Manager component was installed. If the Configuration Manager configuration repository database is not also on this same machine, then copy the scripts to the computer where the database is installed.

5. Uninstall the Configuration Manager Endpoint Extension components from all the gateways. This prevents the code from being downloaded to the endpoints. See "Uninstalling the license management extension components" on page 103.
6. Uninstall the Tivoli License Manager agent bundle component from all the gateways. See "Uninstalling the license management extension components" on page 103.
7. Uninstall the License Compliance Manager agent from the endpoints. See "Uninstalling the agent from the endpoint" on page 104.
8. To remove the Tivoli Management Framework objects that were created in your environment to deploy agents using Configuration Manager software package blocks, run the following script. This is the same script that was run to create the objects.

   ```
   agt_install.pl -uninst
   ```

The two product environments are now standalone and work independently of each other.

Unfederating the databases

This section describes how you can remove the federation of the Configuration Manager configuration repository database and the License Compliance Manager administration server database.

The database federation involves a set of components installed on the License Compliance Manager administration server database. Before removing the federation, ensure that the replica process are not running. See "Stopping and starting the replica processes" on page 52. You remove the federation from the administration server database by running the following script. To run the script, you must be the License Compliance Manager administration server DB2 database instance owner.

Windows
uninstallfed.bat

UNIX uninstallfed.sh

After running the script, the software catalog is no longer copied from the administration server database to the Configuration Manager configuration repository database.

Note: If you were required to install the WebSphere Information Integrator, this script does not remove it.

Uninstalling the license management extension components

This section describes how you can remove the license manage extension components from your Configuration Manager environment.

The following sections explain the uninstallation of the following components:

- Configuration Manager Extension for License Manager installed on the Tivoli server.
- Configuration Manager Endpoint Extension installed on gateways.
- Tivoli License Manager agent bundle installed on gateways.

The Tivoli Management Framework provides a command line utility to remove Tivoli product components from a specified machine or from the entire Tivoli region. The **wuninst** command is a wrapper script that invokes product-specific scripts for uninstalling components. See *Tivoli Management Framework Reference Manual* for detailed information about the **wuninst** command.

The **wuninst** command has the following syntax:

```
 wuninst tag node_name [–rmfiles] [–all]
```

where:

tag Specifies the registered product tag for the component to be uninstalled. To determine the tag for a specific component, use the wuninst –list command. The following are the product tags for the Configuration Manager license management extension components:

Table 23. Product tags for Configuration Manager license management extension components

Component name	**Tag**
Configuration Manager Extension for License Manager	tlm_ext
Configuration Manager Endpoint Extension	cm_ext
Tivoli License Manager agent bundle	tlm_agent

node_name
Specifies the managed node to which this request is directed. This can be any managed node in the region. If you specify the Tivoli server, the actions take place on all managed nodes in your region.

–rmfiles
Deletes binaries, libraries, man pages, objects, methods, and potentially other files associated with the product.

–all Removes the product from the entire Tivoli region

After uninstalling a component, use the wchkdb –ux command to update the Tivoli object database.

For example, the following commands uninstall the Configuration Manager Extension for License Manager and remove the associated file from the Tivoli server oak, and then update the Tivoli object database:

```
wuninst tlm_ext oak -rmfiles
wchkdb -ux
```

Uninstalling the agent from the endpoint

Use the same type of method you chose to deploy agents on your endpoints to remove them. The following two methods are available to uninstall agents from endpoints.

Configuration Manager software package blocks
If you deployed agents on your endpoints by distributing a software package, you can perform a remove change management operation on the agent to uninstall the agent software package.

Inventory dependencies
If you installed the agents using the Inventory dependency method, then launch the appropriate script from the endpoint:

Windows
tlmunins.bat

UNIX tlmunins.sh

These scripts are is located in the path $LCF_DATDIR/../../itlm.

To run this script globally on a group of endpoints at a time, specify the script in an execute program action in a software package and distribute it to the endpoints.

Chapter 14. Supporting partitioning and sub-capacity licenses

This topic describes how you can change your Configuration Manager license management extension environment to support partitioning and sub-capacity licenses.

To support the partitioning and sub-capacity license scenarios, you have the following options:

- "Coexistence between limited and full version of License Compliance Manager."
- "Expanding the limited implementation to the full version."

Coexistence between limited and full version of License Compliance Manager

This topic describes the coexistence between the limited license management extension and the full version of License Compliance Manager.

You can configure the License Compliance Manager administration server to manage not only agents connected to the Tivoli management region server using the Configuration Manager infrastructure, but also License Compliance Manager agents connected using the License Compliance Manager runtime server.

You might want manage agents connected to a runtime server for the following reasons:

- To support sub-capacity licensing scenarios. Refer to *IBM Tivoli License Compliance Manager: Administration* for sub-capacity licensing scenarios.
- To support virtualized environments (VMware and Microsoft® Virtual Server) and partitioned systems on agents. Refer to supported partitioning technologies for agents documented in *IBM Tivoli License Compliance Manager: Planning, Installation, and Configuration*.

Sub-capacity licensing, virtualized environments and partitioned systems on agents can only be supported through the use of a runtime server to which agents connect.

To install a License Compliance Manager runtime server and have agents plug in to it, refer to *IBM Tivoli License Compliance Manager: Planning, Installation, and Configuration*.

Expanding the limited implementation to the full version

This topic describes how you can move from the limited implementation of License Compliance Manager to the full version, to take advantage of all the features and benefits of the product.

Before you begin

You can expand the Configuration Manager license management extension to the IBM Tivoli License Compliance Manager full version. This implies that License Compliance Manager and Configuration Manager no longer work together, but continue to share the same software catalog. The license management extension agents must be migrated to the License Compliance Manager classic agents.

About this task

To upgrade to the stand-alone solution, you need to upgrade or uninstall some components. Perform the following steps to upgrade the solution:

1. To migrate the license management extension agents to the License Compliance Manager classic agents, change the following communication parameters defined in the tlmagent.ini file to communicate with the runtime server:
   - Set the communication type to 1 (this value corresponds to HTTP communication).
   - Runtime server name

   You can change the configuration parameters of an agent by distributing software package blocks provided with the IBM Tivoli License Compliance Manager installation images. The parameters that you can modify are: **server**, **communication_type**, **port**, **use_proxy**, **proxy**, **proxy_port**, **secure_port**, **security_level**, **division**, **scan_exclude_dirs**, and **clear_cache**. You need only to modify the **server** and **communication_type** parameters to migrate Configuration Manager license management extension agents to classic agents. Define the new setting for the SPB on the related platform. When the distribution is complete, ensure that the agents plug in successfully to the runtime server.
2. Migrate the administration server to the classic License Compliance Manager server. In the system.properties configuration file, set the parameter **integrationMode** = `false` after you have verified that all agents have plugged into the License Compliance Manager infrastructure. Restart the server to implement the changes.
3. Remove the database federation by launching the uninstallfed.sh/.bat script. Before launching the script, stop the Apply and Capture replica services. See “Stopping and starting the replica processes” on page 52. For information about running the scripts, see “Unfederating the databases” on page 102.
4. On the computer where the Configuration Manager configuration repository database is installed, run the appropriate script to remove the database federation. You must be the database instance owner to run the script.
   - inv_undo_db2_fed_schema.sql
   - inv_undo_ora_fed_schema.sql

   The script files are located in the path $BINDIR/TME/TLM_EXT/SCRIPTS on the computer where the Configuration Manager Extension for License Manager component was installed. If the Configuration Manager configuration repository database is not also on this same machine, then copy the scripts to the computer where the database is installed.
5. Uninstall the Configuration Manager Extension for License Manager component using the traditional Tivoli uninstallation methods.
6. Uninstall the Configuration Manager Endpoint Extension and the Tivoli License Manager agent bundle, Version 2.3 fix pack 4 component using the traditional Tivoli uninstallation methods. See “Uninstalling the license management extension components” on page 103.

What to do next

At the completion of these steps, both Configuration Managerand License Compliance Manager work independently of each other.

Appendix A. Messages

This section contains the messages generated and logged by Configuration Manager and License Compliance Manager. The messages are divided into the following sections:

-
- “Configuration Manager messages”
- “License Compliance Manager messages” on page 113

Configuration Manager messages

This section contains the messages generated and logged by Configuration Manager license management extension and by the Inventory component. They are divided into the following categories:

- “Configuration Manager Extension for License Manager”
- “Inventory” on page 111

Configuration Manager Extension for License Manager

DISLM1003W No Tivoli License Manager server address has been specified. The delivery of data to the Tivoli License Manager is disabled.

Explanation: You have not specified a value for the **tlm_server_name** paramter in the tlm_extension.ini file.

Operator response: Open the %DBDIR%/tlm_hanlder/tlm_extension.ini file and set a correct value for the **tlm_server_name** parameter.

DISLM1005E A communication error occurred while trying to contact the Tivoli License Manager Administration server. The server may be down or the communication parameters have not been set correctly.

Explanation: The Tivoli License Manager Extension cannot communicate with the Tivoli License Manager Administration server. This might be due to network problems, incorrect communication parameters specified in the tlm_extension.ini file, or to the Tivoli License Manager Administration server being down.

Operator response: Check that the Tivoli License Manager is up and running, that the communication parameters specified in the tlm_extension.ini file are correct, and that the network connectivity is working properly.

DISLM1007E A logic error occurred while trying to send a package with ID *ID_value* to the Tivoli License Manager Administration server.

Explanation: The Tivoli License Manager Extension encountered a logical error while trying to communicate with the Tivoli License Manager Administration server.

Operator response: Check the Tivoli License Manager Administration server log files to investigate the problem.

DISLM1008E A not well defined error occurred while trying to register with the Tivoli License Manager Administration server.

Explanation: The Tivoli License Manager Extension was not able to register with the Tivoli License Manager Administration server.

Operator response: Check the Tivoli License Manager Administration server log and trace files and the Tivoli License Manager Extension log and trace files to investigate the problem.

DISLM1010W The file *file_name* has been discarded because it is a duplicate.

Explanation: A duplicate file was received from a License Compliant Manager agent and the Tivoli License Manager Extension has discarded it. This might happen during a recovery operation performed by a License Compliant Manager agent to avoid losing generated data.

Operator response: No operation is required. The Tivoli License Manager Extension automatically solves the problem.

DISLM1011E The package with ID *ID_value* has been discarded because the Tivoli License Manager Data Handler was not able to deliver it to the Tivoli License Manager Administration server.

Explanation: The maximum number of unsuccessful attempts to deliver a package to the Tivoli License Manager Administration server has been reached. In this case, the package is automatically discarded by the Tivoli License Manager Extension.

Operator response: No operation is required. The Tivoli License Manager Extension automatically solves the problem.

DISLM1012W The configuration parameter *parameter_name*, specified in the file *file_name*, has been forced to *value* because its current value is out of range or is incorrectly specified or is not specified at all.

Explanation: One of the parameters in the specified configuration file is not correctly specified or is missing.

Operator response: Open the specified configuration file and correct the value of the incorrect parameter or add the parameter if missing.

DISLM1014E The agent file *file_name* has been discarded because it is not valid or it is corrupted.

Explanation: The Tivoli License Manager Extension server received a file from a License Compliant Manager agent that is not syntactically correct. The file has been discarded.

Operator response: The Tivoli License Manager Extension automatically solves the problem. Check that the agent that sent the corrupted file is working correctly.

DISLM1015E An error occurred while the Tivoli License Manager Data Handler was preparing a package with ID *ID_value*. The package will be discarded.

Explanation: A problem occurred on the file system where the %DBDIR%/tlm_handler directory is located.

Operator response: Check that there is enough space available on the specified file system and that the file system is working correctly.

DISLM1017E The Tivoli License Manager Data Handler engine was unable to start. The following error occurred: *error_message*.

Explanation: The Tivoli License Manager Extension server encountered an error while starting.

Operator response: Check the log and trace files located in the %DBDIR%/tlm_handler/log directory.

DISLM1018E The registration with the Tivoli License Manager Administration server completed with errors. The server has not been recognized. Check that the tlm_runtime_name parameter has been set to a correct value.

Explanation: The Tivoli License Manager Extension was not able to register with the Tivoli License Manager Administration server because it was not recognized as a valid server.

Operator response: Verify the value of the **tlm_runtime_name** parameter in the tlm_extension.ini configuration file. This value should match the name specified in the Tivoli License Manager Administration server GUI for the server representing the Tivoli server.

DISLM1019E A communication error occurred while trying to send a package with ID *ID_value* to the Tivoli License Manager Administration server. The server may be down or the content of the package may be incorrect.

Explanation: The Tivoli License Manager Extension encountered a communication error while sending a data package to the Tivoli License Manager Administration server. The Tivoli License Manager Administration server might be down or the package might be corrupt.

Operator response: Check whether the Tivoli License Manager Administration server is up and running, the network is working properly, and the package was created properly.

DISLM1020E A logic error with return code *return_code* occurred contacting the License Compliance Manager server.

Explanation: The following is a list of the return codes and a possible cause and solution for each code:

Table 24. Return codes

Return Code	Cause	Solution
0	Successful	

Table 24. Return codes (continued)

Return Code	Cause	Solution
-8	The package with ID *ID_value* has been discarded because it has already been delivered to the License Compliance Manager administration server.	
-501	The registration with the License Compliance Manager administration server completed with errors. The server has not been recognized.	Check that the tlm_runtime_name parameter has been set to a correct value. You can verify the value of the parameter in the tlm_extension.ini configuration file.
-503	Information about the node or the agent are inconsistent according to the information currently stored in the administration server database. Maybe the request has been corrupted or the administration server database altered.	Contact IBM support.
-506	a download catalog service has been requested to the Admin Server when the catalog manager has run since less than 5 minutes	Try again in 5 minutes.
-599	An internal technical error has occurred while the administration server was executing the business logic.	Contact IBM support.

Operator response: See explanation for possible solutions.

DISLM1021E A generic error occurred running the specified operation.

Explanation: The command encountered an unexpected error.

Operator response: Check the Tivoli License Manager Extension log and trace files to investigate the problem.

DISLM1023E The following error occurred pushing the requested information to agents: *error_message***.**

Explanation: The command failed while invoking the **winstsp** command. A more specific error message is displayed in association with this message.

Operator response: Check the Configuration Manager message as a starting point to investigate the problem

DISLM1024E The Tivoli License Manager Data Handler engine was unable to find the data for the service *service_name* **on the License Compliance Manager Server.**

Explanation: The command failed while trying to download the signature catalog from the Tivoli License Manager Administration server.

Operator response: Check on the Tivoli License Manager Administration server if the signature catalog has been correctly generated. Additionally check the Tivoli License Manager Administration server log and traces to investigate the problem.

DISLM1025E The Tivoli License Manager Data Handler engine was unable to write the data for the service *service_name* **on the License Compliance Manager Server.**

Explanation: The command failed while downloading data from the Tivoli License Manager Administration server.

Operator response: Check that there is enough space available on the file system where the directory %DBDIR%/tlm_handler is located and that the communication with the Tivoli License Manager Administration server is working correctly

DISLM1103E The command completed with errors. Check logs and traces to determine the problem.

Explanation: The command has encountered an unexpected error. This message is usually displayed in association with a more precise error message which explains the cause of the failure in more detail.

Operator response: Check the License Management Extension log and trace files.

DISLM1104E The command failed. Unable to determine the value of the BINDIR environment variable.

Explanation: You have issued a CLI command in a shell where the Tivoli environment was incorrectly configured.

Operator response: Check that your Tivoli environment is correctly configured.

DISLM1105E The requested operation failed. Error message: *error_message***.**

Explanation: The command encountered an unexpected error.

Operator response: Check the associated message to understand the cause of the failure. If the information is not sufficient, check logs and traces in the %DBDIR%/tlm_handler/log directory.

DISLM1108E Unable to create or manage *directory_name* **directory.**

Explanation: The command failed because it cannot create the specified directory.

Operator response: Check that the user issuing the command has the correct permissions to create the specified directory.

DISLM1109E The file *file_name* **does not exist or is empty.**

Explanation: The file you have specified is either incorrect or does not exist.

Operator response: Type the command again specifying a correct value for the file name.

DISLM1110E *Profile_manager_name* **is not a profile manager or is empty.**

Explanation: The profile manager name you specified is either incorrect or the profile manager is empty.

Operator response: Type the command again specifying a correct value for the profile manager name.

DISLM1111E A problem occurred trying to create software package *software_package_name***.**

Explanation: The command failed in re-creating the specified software package.

Operator response: Check that the user issuing the command has the correct role to perform the operation. The requested role is senior. Also check the logs and traces in the %DBDIR%/tlm_handler/log directory.

DISLM1112E *Endpoint_name* **is not a valid endpoint.**

Explanation: The **wtlminfoget** command failed because one of the endpoints you specified as an input parameter is not valid.

Operator response: Type the command again specifying a correct value for the endpoint.

DISLM1113E No target is specified or no target qualified for the operation.

Explanation: The command failed because you have not specified a valid target for the requested operation.

Operator response: Type the command again specifying a correct value for the target.

DISLM1114W Some of the targets specified for the operation are not valid.

Explanation: The **wtlminfoget** command discovered that some of the specified targets are not valid for the requested operation but the **continue_on_invalid_targets** parameter was set to **yes** using the **wswdcfg** command.

Operator response: No operation is required. The operation continues only on the valid targets.

DISLM1115E Invalid pathname *path_name***. Absolute path is required.**

Explanation: The path name you have specified is incorrect.

Operator response: Provide the absolute path to the file.

DISLM1117E No valid input value for timeout.

Explanation: You have specified an incorrect value for the **timeout** parameter of the **wtlmdh** command.

Operator response: Type the command again specifying a correct value for the **timeout** parameter.

ISLM1118E *Managed_node_name* **is not a managed node.**

Explanation: The managed node name you have specified is incorrect.

Operator response: Type the command again specifying a correct value for the managed node name.

DISLM1119E The License Manager data handler already exists on this Tivoli server.

Explanation: The License Manager extension is already existing on the specified managed node.

Operator response: The License Manager extension is already existing on the server and you do not need to create a new one. To move the extension to a new managed node, use the **-m** *managed_node* option.

DISLM1120E Destination dispatcher unavailable.

Explanation: The managed node where the user is trying to move or create the License Compliance Manager Data Handler cannot be reached.

Operator response: Check that the Tivoli License Manager is up and running and that the network connectivity is working properly.

DISLM1121E License Manager data handler creation ERROR: ***error_message*.**

Explanation: The system cannot create the License Compliance Manager Data Handler. The associated error message contains more information.

Operator response: Check the associated message to understand the cause of the failure. If the information is not sufficient, check logs and traces in the %DBDIR%/tlm_handler/log directory.

DISLM1122E Error accessing the License Manager Data Handler.

Explanation: This error is usually it is associated with an incorrect configuration of the Tivoli environment or an incorrect installation of the product.

Operator response: Check if the Tivoli environment is up and running and if the Tivoli License Manager Extension component is correctly installed.

DISLM1123E The License Manager data handler does not exist on host ***host_name*.**

Explanation: The host name you specified is incorrect.

Operator response: Type the command again specifying a correct value for the host name.

ISLM1124E The License Manager data handler does not exist.

Explanation: The License Compliance Manager Data Handler is not installed on the specified node.

Operator response: Type the command again specifying a correct value for the node name.

DISLM1128E The Configuration Manager Extension for License Manager is not installed on ***managed_node_name*.**

Explanation: You are trying to create or move the License Compliance Manager Data Handler from or on a node.

Operator response: Install the Configuration Manager Extension for License Manager on the managed node where you are trying to create or move the License Compliance Manager Data Handler.

DISLM1129E Unable to force the processing of the remaining License Manager data files present in the depot directory of the Configuration Manager Extension for License Manager component. See the Configuration Manager Extension for License Manager log file for additional details about this error.

Explanation: The system cannot stop the License Compliance Manager Data Handler.

Operator response: Check logs and traces in the %DBDIR%/tlm_handler/log directory of the machine where the License Compliance Manager Data Handler is currently active.

DISLM1130E The Configuration Manager Extension for License Manager component is disabled on this node. Operation unsuccessful.

Explanation: You are trying to run a command on a managed node where the Configuration Manager Extension for License Manager is not active. By default, the Configuration Manager Extension for License Manager is active on the Tivoli server. You can move the Configuration Manager Extension for License Manager to a different node using the **wtlmdh** command.

Operator response: Move to a managed node where the Configuration Manager Extension for License Manager is active and type the command again.

Inventory

INVTS0001E File catman.ini not found.

Explanation: The catman.ini file contains information the Tivoli License Manager Catalog Manager installation on the machine. If the file is missing, an error was probably encountered while installing this component or the file was manually deleted.

Operator response: Check that the installation of the Tivoli License Manager Catalog Manager completed successfully. If the installation was successful, manually recreate the catman.ini file. The file is located in the following path:

On UNIX systems
/etc

On Windows systems
%SystemRoot%

The file should contain just one line with the following format: `catimp_path=`*`TTLM_Catalog_Manager_bin_dir`*.

INVTS0002E Key *key_name* **not found.**

Explanation: A problem occurred while parsing the catman.ini file. Because the file does not contain the specified key, it might be corrupt.

Operator response: Open the catman.ini file and correct the problem by reinserting the missing key.

INVTS0003E Error accessing table *table_name***.**

Explanation: A problem occurred while a signature was being inserted in the Tivoli Configuration Manager database. The database schema might be wrong or corrupted.

Operator response: Check the Tivoli Configuration Manager database schema was correctly updated.

INVTS0004E Error catalog manager *parameter_name* **not defined**

Explanation: The system is unable to retrieve the specified parameter and call the Tivoli License Manager Catalog Manager

Operator response: Check that the username and password to access the Tivoli License Manager Catalog Manager have been correctly set using the **winvsig** command.

INVTS0005E Error returned from catalog manager *error_message***.**

Explanation: A problem occurred while invoking the Tivoli License Manager Catalog Manager. The associated error message contains more information.

Operator response: Check the associated error message and take the appropriate actions.

INVCO0019W The import of the signature catalog into the Tivoli License Manager agent failed with return code: *error_code*

Explanation: A problem occurred while importing a signature catalog to the Tivoli License Manager agent.

Operator response: Check the error code and take the appropriate actions. See the return codes related to the ITLMInfo.1 software package.

INVCO0020W It was not possible to start the command to import the catalog to the License Manager agent.

Explanation: A problem occurred while trying to invoke the Tivoli License Manager agent command line to import the signature catalog.

Operator response: Check that the Tivoli License Manager agent is correctly installed.

INVCO0021W The export of the signature catalog from the License Manager agent failed with return code : *error_code*

Explanation: A problem occurred while exporting a signature catalog from the Tivoli License Manager agent.

Operator response: Check the error code and take the appropriate actions. See the return codes related to the ITLMInfo.1 software package.

INVCO0022W Inventory was unable to export the signature catalog from the License Manager agent. An unspecified error occurred.

Explanation: A problem occurred trying to invoke the Tivoli License Manager agent command line to export the signature catalog.

Operator response: Check that the Tivoli License Manager agent is correctly installed.

INVCO0023W The License Manager agent is not running. It must be started before any operation can be requested.

Explanation: The License Manager agent is not running.

Operator response: Restart the License Manager agent. To perform this operation, you can use the startITLMAgent.1 software package or you can start the agent manually.

INVCO0024W The License Manager agent is not installed.

Explanation: The License Manager agent seems to be not installed because its command line is not available on the agent.

Operator response: Check if the License Manager agent is correctly installed.

INVCO0025W File or directory *file_name* **does not exist; License Manager Agent installation cannot be performed.**

Explanation: You cannot install the License Manager agent because one of the files required for the installation is missing. This problem might occur if the Tivoli License Manager agent has not been correctly installed on the gateways.

Operator response: Check that the Tivoli License Manager agent has been correctly installed on the gateway.

INVCO0026W Operating system is not supported by License Manager Agent.

Explanation: You are trying to install the License Manager agent on an unsupported platform.

Operator response: Exclude the specified endpoint from the machines where the License Manager Agent is to be installed.

INVCO0027W The License Manager agent installation might not be started or has timed out.

Explanation: The system is unable to start the installation of the License Manager agent or the installation timed out.

Operator response: Check the License Management Extension log and trace files.

INVCO0028W Tivoli License Manager Agent installation failed with return code: *error_code***.**

Explanation: The installation of the Tivoli License Manager Agent failed with the specified return code.

Operator response: Check the reported error code on the *IBM Tivoli License Manager: Problem Determination* and take the appropriate actions.

INVCO0029W An error occurred running command *command_name***, return code =** *return_code***. Failure of this command prevents Upload Manager from resolving dependencies and synchronizing data.**

Explanation: The Upload Manager component was unable to run the specified command.

Operator response: Check the specified error code for the given command on the manual of the corresponding application: *User's Guide for Inventory* or *IBM Tivoli License Manager: Problem Determination*.

INVCO0030W The import of the signature catalog to the License Manager agent failed because the catalog is older than the existing catalog.

Explanation: You are trying to import an older catalog into the License Manager agent. This might occur if you are pushing a software Inventory scan with signatures on a machine where the same catalog has already been imported.

Operator response: No action should be taken if you are pushing an Inventory scan with a catalog already imported in the License Manager agent. Otherwise, update the version of the catalog that you are trying to import in the License Manager agent.

INVCO0031W Tivoli License Manager agent was not installed because an agent is already present and it is not configured to work with Configuration Manager.

Explanation: The system is trying to install a Tivoli License Manager agent on a workstation where an agent is already installed but configured not be to integrated with Tivoli Configuration Manager.

Operator response: If you want to manage that machine with the integrated solution you need to uninstall the current version of the agent and install an integrated one.

License Compliance Manager messages

This section contains the messages generated and logged by License Compliance Manager in the Configuration Manager license management extension evironment. The messages are divided into the following categories:

- "Server and database installation messages"
- "Server command-line messages" on page 115
- "Agent messages" on page 116

Refer to *IBM Tivoli License Compliance Manager: Problem Determination* for messages generated and logged by IBM Tivoli License Compliance Manager

Server and database installation messages

CODIN0197E Error verifying the configuration parameters for the database federation. Ensure that the database configuration parameters, FEDERATED and LOGRETAIN, are set correctly.
Refer to the documentation for further information.

Explanation: The values of the database configuration parameters that enable the federation might not be set correctly.

Operator response: See message text.

CODIN0198E Error running cleanup script for the administration server database. Refer to trace_db_servers_uninstall.log log file for further information.

Explanation: See message text.

Operator response: See message text.

CODIN0199E Error running the removal of the database federation. Refer to the trace_db_servers_uninstall.log log file for further information.

Explanation: See message text.

Operator response: See message text.

CODIN0200W The federation process Apply and Capture have been started on your computer. If you want to register Apply and Capture as services refer to the documentation.

Explanation: See message text.

Operator response: See message text.

CODIN0201W Verify that the federation services Apply and Capture have been removed correctly. Refer to the documentation for further information.

Explanation: See message text.

Operator response: See message text.

CODIN0202E There are no elements of the Tivoli License Manager infrastructure installed on this computer.

Explanation: See message text.

Operator response: See message text.

CODIN0203E The ITCM catalog has not been migrated. Run the winvmigrate command on Inventory TMR. Refer to documentation for further information.

Explanation: See message text.

Operator response: See message text.

CODIN0204W An error occurred while attempting to uncatalog the inventory configuration repository.

Explanation: See message text.

Operator response: Click "Finish" to exit, and uncatalog the database manually.

CODIN0209W The installation process will set the TLMA database logging type from “Manual logging” to “Archive logging”. By default, the DB2 transaction logs will not be archived automatically.

Explanation: See message text.

Operator response: Refer to the DB2 Administration Guide to change this setting.

Server command-line messages

CODCL7524E The agent ID: {0} is assigned to multiple divisions as follows: {1}.

Explanation: The input XML file contains an agent ID that is assigned to more than one division.

Operator response: Correct the XML file so that the agent ID is assigned to only one division and retry the command.

CODCL7525E The Tivoli object ID: {0} is assigned to multiple divisions as follows: {1}.

Explanation: The input XML file contains a Tivoli object ID that is assigned to more than one division.

Operator response: Correct the XML file so that the Tivoli object ID is assigned to only one division and retry the command.

CODCL7526E The agent ID: {0} appears to be assigned to a different division: {1} than another Tivoli object ID.

Explanation: The command converts the Tivoli object ID into an agent ID. It might occur that the converted agent ID is identical to an agent ID already present in the XML file, and the two agent IDs are assigned to different divisions.

Operator response: To resolve the conflict, query the database to identify the Tivoli object ID that corresponds to the conflicting agent ID, and then search the XML file for the same agent ID mapped to a different division.

CODCL7527E The Tivoli object ID: {0} was not found in the database.

Explanation: One possible cause is that an editing mistake was made when the OID was specified in the XML file. A second possibility is that in the intervening period between querying the administration server database and running the command, the Tivoli endpoint was removed and the OID deleted from the database.

Operator response: Check the XML for errors in the way in which the Tivoli OID was specified and correct it. If the Tivoli OID is specified correctly in the XML file, check the administration server database to verify that the endpoint has been deleted and then remove it from the file.

CODCL7528E The agent ID: {0} does not belong to the default division.

Explanation: You cannot remap an agent that has already been remapped. To remap an agent, it must be assigned to the default division.

Operator response: Remove the agent ID from the input XML file.

CODCL7529E The agent ID: {0} could not be written to the administration server database.

Explanation: An error has occurred accessing the administration server database.

Operator response: Check the trace and log files for details to correct the problem, and retry the command.

Agent messages

CODAG043E The agent could not connect to the runtime server because of internal problems.

Explanation: The agent and runtime server are not correctly aligned. The problem will be resolved by an internal process.

Operator response: Wait for the agent to automatically retry the connection.

CODAG044E The import command has failed because the specified input file cannot be found.

Explanation: The file you have specified does not exist.

Operator response: Check the file name and path that you have specified and retry the command.

CODAG045E The import command has failed.

Explanation: It is possible that the specified file is not a valid catalog or that a technical error has occurred.

Operator response: Check that the file you specified is a catalog file and retry the command. If the problem persists contact IBM Software Support.

CODAG046E The export command has failed.

Explanation: A technical error has occurred.

Operator response: Contact IBM Software Support.

CODAG047E The export command has failed because the output file could not be created.

Explanation: The catalog export file could not be created in the path that you specified.

Operator response: Ensure that you have sufficient permissions to write to the specified directory and that there is sufficient space available, then retry the command.

CODAG048E The catalog file has not been imported because the specified file is not valid.

Explanation: Either the current agent catalog is more recent than the file you specified, or the size of the specified file is 0.

Operator response: No action is required until an updated catalog is distributed.

CODAG049E The software inventory scan failed to complete successfully.

Explanation: Common Inventory Technology (CIT) component encountered an error and could not complete the scan.

Operator response: Check the agent and the CIT trace logs for information and retry the scan.

CODAG050E The hardware scan failed to complete successfully.

Explanation: Common Inventory Technology (CIT) component encountered an error and could not complete the scan.

Operator response: Check the agent and the CIT trace logs for information and retry the scan.

CODAG051E The scan failed while performing the agent plugin.

Explanation: The agent has failed to invoke the Configuration Manager Endpoint Extension component and could not upload the scan to the server.

Operator response: Verify that the Configuration Manager Endpoint Extension component is installed and functioning correctly and retry the scan.

CODAG052E The scan failed while performing the agent data upload.

Explanation: The scan information has not been transferred possibly because of a network error or an error in the Configuration Manager Endpoint Extension component.

Operator response: Check the agent trace log and the Configuration Manager Endpoint Extension component log and retry the scan.

CODAG053E The command cannot run because the agent is busy performing another activity.

Explanation: See message text.

Operator response: Retry the command later.

CODAG054E The parameter you are attempting to change does not exist in the agent configuration file.

Explanation: This is not a valid agent parameter.

Operator response: Check that the parameter has been correctly specified.

CODAG055E The parameter you are attempting to change is not reloadable.

Explanation: Only reloadable parameters can be changed using this command.

Operator response: If you need to change this parameter, edit the agent configuration file and restart the agent.

CODAG056E The value you specified for the parameter is not a valid value.

Explanation: See message text.

Operator response: Verify the acceptable values for the parameter and retry the command.

Appendix B. Support information

If you have a problem with your IBM software, you want to resolve it quickly. This section describes the following options for obtaining support for IBM software products:

- "Using IBM Support Assistant"
- "Obtaining fixes"
- "Receiving weekly support updates" on page 120
- "Contacting IBM Software Support" on page 121

Using IBM Support Assistant

The IBM Support Assistant is a free, stand-alone application that you can install on any workstation. You can then enhance the application by installing product-specific plug-in modules for the IBM products you use.

The IBM Support Assistant saves you time searching product, support, and educational resources. The IBM Support Assistant helps you gather support information when you need to open a problem management record (PMR), which you can then use to track the problem.

The product-specific plug-in modules provide you with the following resources:

- Support links
- Education links
- Ability to submit problem management reports

If your product does not use IBM Support Assistant, use the links to support topics in your information center. In the navigation frame, check the links for resources listed in the **ibm.com® and related resources** section where you can search the following resources:

- Support and assistance (includes search capability of IBM technotes and IBM downloads for interim fixes and workarounds)
- Training and certification
- IBM developerWorks®
- IBM Redbooks®
- General product information

If you cannot find the solution to your problem in the information center, search the following Internet resources for the latest information that might help you resolve your problem:

- Forums and newsgroups
- Google.com

Obtaining fixes

A product fix might be available to resolve your problem. To determine what fixes are available for your IBM software product, follow these steps:

1. Go to the IBM Software Support Web site at http://www.ibm.com/software/support.

2. Under **Find product support**, click All IBM software (A-Z). This opens the software product list.
3. In the software product list, click **IBM Tivoli Configuration Manager**. This opens the IBM Tivoli Configuration Manager support site.
4. Under **Solve a problem**, click **APARs** to go to a list of fixes, fix packs, and other service updates for IBM Tivoli Configuration Manager.
5. Click the name of a fix to read the description and optionally download the fix. You can also search for a specific fix; for tips on refining your search, click **Search tips**.
6. In the **Find downloads and drivers by product** section, select one software category from the **Category** list.
7. Select one product from the **Sub-category** list.
8. Type more search terms in the **Search within results** if you want to refine your search.
9. Click **Search**.
10. From the list of downloads returned by your search, click the name of a fix to read the description of the fix and to optionally download the fix.

For more information about the types of fixes that are available, see the *IBM Software Support Handbook* at http://techsupport.services.ibm.com/guides/handbook.html.

Receiving weekly support updates

To receive weekly e-mail notifications about fixes and other software support news, follow these steps:

1. Go to the IBM Software Support Web site at http://www.ibm.com/software/support.
2. Click **My support** in the far upper-right corner of the page under **Personalized support**.
3. If you have already registered for **My support**, sign in and skip to the next step. If you have not registered, click **register now**. Complete the registration form using your e-mail address as your IBM ID and click **Submit**.
4. Click **Edit profile**.
5. In the **Products** list, select **Software**. A second list is displayed.
6. In the second list, select a product segment, for example, **Application servers**. A third list is displayed.
7. In the third list, select a product sub-segment, for example, **Distributed Application & Web Servers**. A list of applicable products is displayed.
8. Select the products for which you want to receive updates.
9. Click **Add products**.
10. After selecting all products that are of interest to you, click **Subscribe to email** on the **Edit profile** tab.
11. Select **Please send these documents by weekly email**.
12. Update your e-mail address as needed.
13. In the **Documents** list, select **Software**.
14. Select the types of documents that you want to receive information about.
15. Click **Update**.

If you experience problems with the **My support** feature, you can obtain help in one of the following ways:

Online
Send an e-mail message to erchelp@ca.ibm.com, describing your problem.

By phone
Call 1-800-IBM-4You (1-800-426-4968).

Contacting IBM Software Support

IBM Software Support provides assistance with product defects.

Before contacting IBM Software Support, your company must have an active IBM software maintenance contract, and you must be authorized to submit problems to IBM. The type of software maintenance contract that you need depends on the type of product you have:

- For IBM distributed software products (including, but not limited to, Tivoli, Lotus®, and Rational® products, as well as DB2 and WebSphere products that run on Windows, or UNIX operating systems), enroll in Passport Advantage® in one of the following ways:

  Online
  Go to the Passport Advantage Web site at http://www-306.ibm.com/software/howtobuy/passportadvantage/pao_customers.htm.

  By phone
  For the phone number to call in your country, go to the IBM Software Support Web site at http://techsupport.services.ibm.com/guides/contacts.html and click the name of your geographic region.
- For customers with Subscription and Support (S & S) contracts, go to the Software Service Request Web site at https://techsupport.services.ibm.com/ssr/login.
- For customers with IBMLink™, CATIA, Linux, OS/390®, iSeries, pSeries, zSeries, and other support agreements, go to the IBM Support Line Web site at http://www.ibm.com/services/us/index.wss/so/its/a1000030/dt006.
- For IBM eServer™ software products (including, but not limited to, DB2 and WebSphere products that run in zSeries, pSeries, and iSeries environments), you can purchase a software maintenance agreement by working directly with an IBM sales representative or an IBM Business Partner. For more information about support for eServer software products, go to the IBM Technical Support Advantage Web site at http://www.ibm.com/servers/eserver/techsupport.html.

If you are not sure what type of software maintenance contract you need, call 1-800-IBMSERV (1-800-426-7378) in the United States. From other countries, go to the contacts page of the *IBM Software Support Handbook* on the Web at http://techsupport.services.ibm.com/guides/contacts.html and click the name of your geographic region for phone numbers of people who provide support for your location.

To contact IBM Software support, follow these steps:
1. “Determining the business impact” on page 122
2. “Describing problems and gathering information” on page 122
3. “Submitting problems” on page 122

Determining the business impact

When you report a problem to IBM, you are asked to supply a severity level. Therefore, you need to understand and assess the business impact of the problem that you are reporting. Use the following criteria:

Severity 1
The problem has a *critical* business impact. You are unable to use the program, resulting in a critical impact on operations. This condition requires an immediate solution.

Severity 2
The problem has a *significant* business impact. The program is usable, but it is severely limited.

Severity 3
The problem has *some* business impact. The program is usable, but less significant features (not critical to operations) are unavailable.

Severity 4
The problem has *minimal* business impact. The problem causes little impact on operations, or a reasonable circumvention to the problem was implemented.

Describing problems and gathering information

When describing a problem to IBM, be as specific as possible. Include all relevant background information so that IBM Software Support specialists can help you solve the problem efficiently. To save time, know the answers to these questions:

- What software versions were you running when the problem occurred?
- Do you have logs, traces, and messages that are related to the problem symptoms? IBM Software Support is likely to ask for this information.
- Can you re-create the problem? If so, what steps were performed to re-create the problem?
- Did you make any changes to the system? For example, did you make changes to the hardware, operating system, networking software, and so on.
- Are you currently using a workaround for the problem? If so, be prepared to explain the workaround when you report the problem.

Submitting problems

You can submit your problem to IBM Software Support in one of two ways:

Online
Click **Submit and track problems** on the IBM Software Support site athttp://www.ibm.com/software/support/probsub.html. Type your information into the appropriate problem submission form.

By phone
For the phone number to call in your country, go to the contacts page of the *IBM Software Support Handbook* at http://techsupport.services.ibm.com/guides/contacts.html and click the name of your geographic region.

If the problem you submit is for a software defect or for missing or inaccurate documentation, IBM Software Support creates an Authorized Program Analysis Report (APAR). The APAR describes the problem in detail. Whenever possible, IBM Software Support provides a workaround that you can implement until the APAR is resolved and a fix is delivered. IBM publishes resolved APARs on the

Software Support Web site daily, so that other users who experience the same problem can benefit from the same resolution.

Appendix C. 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 give you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785, U.S.A.

For license inquiries regarding double-byte (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

IBM World Trade Asia Corporation
Licensing
2-31 Roppongi 3-chome, Minato-ku
Tokyo 106, 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 might 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 78758 U.S.A.

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement or any equivalent agreement between us.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurement may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

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.

All statements regarding IBM’s future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. You may copy, modify, and distribute these sample programs in any form without payment to

IBM for the purposes of developing, using, marketing, or distributing application programs conforming to IBM's application programming interfaces.

Each copy or any portion of these sample programs or any derivative work, must include a copyright notice as follows:

© International Business Machines Corporation, 2003. Portions of this code are derived from IBM Corp. Sample Programs. © Copyright IBM Corp. _enter the year or years_. All rights reserved.

If you are viewing this information in softcopy form, the photographs and color illustrations might not appear.

Trademarks

AIX, DB2, DB2® Universal Database™, developerWorks, eServer, i5/OS, IBM, the IBM logo, ibm.com, IBMLink, Informix®, iSeries, Lotus, Notes®, OS/390, OS/400, Passport Advantage, pSeries, Rational, Redbooks, RS/6000®, S/390, SecureWay®, Tivoli, Tivoli Enterprise, Tivoli Enterprise Console®, the Tivoli logo, WebSphere, z/OS®, and zSeries are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both.

Intel, Intel Inside® (logos), MMX, Celeron®, Intel Centrino®, Intel Xeon®, Itanium®, Pentium® and Pentium III Xeon are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States, other countries, or both.

Java and all Java-based trademarks and logos are trademarks or registered trademarks of Sun Microsystems, Inc. in the U.S., and other countries, or both.

Linux is a trademark of Linus Torvalds in the United States, other countries, or both.

Microsoft, Windows, and the Windows logo are registered trademarks, of Microsoft Corporation in the U.S. and other countries.

SSLRef 1.0 is a trademark of Netscape Communications Corporation.

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

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

Index