IBM Tivoli Asset Discovery for Distributed
Version 7.2.2

Installing IBM Tivoli Asset Discovery for Distributed 7.2.2 on embedded WebSphere Application Server

IBM
Installing IBM Tivoli Asset Discovery for Distributed 7.2.2 on embedded WebSphere Application Server
Installation Guide

This edition applies to version 7.2.2 of IBM Tivoli Asset Discovery for Distributed (product number 5724-S94) and to all subsequent releases and modifications until otherwise indicated in new editions.

US Government Users Restricted Rights – Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.
<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Installing agents on Solaris using native installers</td>
<td>113</td>
</tr>
<tr>
<td>Installing agents interactively</td>
<td>113</td>
</tr>
<tr>
<td>Installing agents on Windows using a native installer</td>
<td>115</td>
</tr>
<tr>
<td>Installing agents interactively</td>
<td>115</td>
</tr>
<tr>
<td>Installing agents silently</td>
<td>118</td>
</tr>
<tr>
<td>Rerunning a failed agent installation</td>
<td>118</td>
</tr>
<tr>
<td>Rerunning agent installation that failed in the preinstallation phase</td>
<td>119</td>
</tr>
<tr>
<td>Rerunning agent installation that failed in the postinstallation phase</td>
<td>119</td>
</tr>
<tr>
<td>Installing agents on UNIX using shell installers</td>
<td>120</td>
</tr>
<tr>
<td>Using IBM Tivoli Configuration Manager to install the agents in bulk</td>
<td>121</td>
</tr>
<tr>
<td>Software package parameters</td>
<td>123</td>
</tr>
<tr>
<td>Installing agents with Windows logon scripts</td>
<td>125</td>
</tr>
<tr>
<td>Performing a refresh installation of agents</td>
<td>127</td>
</tr>
<tr>
<td>Image cloning with preinstalled agents</td>
<td>128</td>
</tr>
<tr>
<td>Agent installation response files</td>
<td>129</td>
</tr>
<tr>
<td>Windows agent installation response file and logon script configuration file</td>
<td>129</td>
</tr>
<tr>
<td>UNIX agents installation response file</td>
<td>131</td>
</tr>
<tr>
<td>IBM i agent installation response file</td>
<td>134</td>
</tr>
<tr>
<td>Troubleshooting agent installation and uninstallation</td>
<td>136</td>
</tr>
<tr>
<td>Agent installation problems on AIX platforms</td>
<td>136</td>
</tr>
<tr>
<td>Agent installation problems on Linux operating system</td>
<td>137</td>
</tr>
<tr>
<td>Agent installation problems on IBM i, Windows and Solaris platforms</td>
<td>139</td>
</tr>
<tr>
<td>Agent upgrade and self-update problems</td>
<td>140</td>
</tr>
<tr>
<td>Other agent installation problems</td>
<td>140</td>
</tr>
<tr>
<td>Disabling rollback of failed agent installations</td>
<td>142</td>
</tr>
<tr>
<td>Chapter 4. Uninstalling</td>
<td>145</td>
</tr>
<tr>
<td>Uninstalling the Tivoli Asset Discovery for Distributed servers and databases</td>
<td>145</td>
</tr>
<tr>
<td>Uninstalling the server in interactive mode</td>
<td>145</td>
</tr>
<tr>
<td>Uninstalling the server in silent mode</td>
<td>146</td>
</tr>
<tr>
<td>The server and database uninstallation response file</td>
<td>147</td>
</tr>
<tr>
<td>Running scripts to uninstall Tivoli Asset Discovery for Distributed</td>
<td>148</td>
</tr>
<tr>
<td>Scripts used in undeploying the server on WebSphere Application base version</td>
<td>149</td>
</tr>
<tr>
<td>Uninstalling agents</td>
<td>149</td>
</tr>
<tr>
<td>Uninstalling Tivoli Asset Discovery for Distributed agents using the tlmunins script</td>
<td>149</td>
</tr>
<tr>
<td>Uninstalling agents using native installation tools</td>
<td>150</td>
</tr>
<tr>
<td>Uninstalling AIX agents</td>
<td>150</td>
</tr>
<tr>
<td>Uninstalling HP-UX agents</td>
<td>150</td>
</tr>
<tr>
<td>Uninstalling IBM i agents</td>
<td>151</td>
</tr>
<tr>
<td>Uninstalling Linux agents</td>
<td>151</td>
</tr>
<tr>
<td>Uninstalling Solaris agents</td>
<td>151</td>
</tr>
<tr>
<td>Uninstalling Windows agents</td>
<td>151</td>
</tr>
<tr>
<td>Notices</td>
<td>153</td>
</tr>
<tr>
<td>Trademarks</td>
<td>154</td>
</tr>
<tr>
<td>Index</td>
<td>157</td>
</tr>
</tbody>
</table>
Chapter 1. Installing IBM Tivoli Asset Discovery for Distributed

Read this guide to learn how to perform the Tivoli® Asset Discovery for Distributed installation.

The following changes in the installation process and packages have been introduced in release 7.2.2:

- InstallAnywhere 2009 installation framework has been implemented (installation wizard),
- installation of DB2® has been removed from the installation wizard,
- the files for manual deployment are now in a separate package (Passport Advantage® download or separate DVD). They cannot be extracted from the wizard.

Introduction

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

Tivoli Asset Discovery for Distributed components

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

Server components

WebSphere Application Server (embedded or base)
- Tivoli Asset Discovery for Distributed server
- DB2 database
- Integrated Solutions Console
- Command-line interface

Agents

© Copyright IBM Corp. 2002, 2010
subscribed users to be notified about events which are relevant to their roles. Each installation of Tivoli Asset Discovery for Distributed has a single server, which can run either on the embedded or base version of the WebSphere® Application Server software.

**Database**

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

**Integrated Solutions Console**

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

**Command-line interface**

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

**Agents**

Agents are installed on each operating system that should be monitored by Tivoli Asset Discovery for Distributed. They perform hardware and software scans and forward the results to the server.
Chapter 2. Installing on embedded WebSphere Application Server

The installation of IBM Tivoli Asset Discovery for Distributed has the following phases: server installation, configuration of the server and the installation of agents.

1. **Plan the installation** Before starting the server installation, review the information in this section to learn about hardware and software requirements and other considerations. (REQUIRED)
2. **Perform preinstallation steps** before you start the installation, prepare installation images. If you want to install the server and database on different server computers, synchronize the administration and database server clocks.
3. If you do not want to reuse an existing instance of the database, **install DB2** (OPTIONAL), either on the same or separate server. For more information about the advantages and disadvantages of each topology, consult “Planning the topology” on page 4.
4. Install the server **interactively** or **silently**.

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

**Silent installation**
Specify parameters in a response file and start the installation from the command line. Use this approach for unattended installation.

Another option is to **install the server in a distributed environment** (with the database on a separate computer). (REQUIRED)
5. **Start web user interface** to verify the installation. (OPTIONAL)
6. **Start troubleshooting** if problems have occurred. (OPTIONAL)
7. **Install Software Knowledge Base Toolkit** and perform a few important steps after the installation. This product is necessary for managing the software catalog. (REQUIRED)
8. **Install Tivoli Common Reporting** (OPTIONAL)

After you have installed the server, **configure** it. The next task is to **install the agents**.

Planning the Tivoli Asset Discovery for Distributed server installation

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

Depending on your needs, you can install the IBM Tivoli Asset Discovery for Distributed server with the embedded or base WebSphere Application Server. You can also consider installing DB2 on a separate server computer.

Procedure

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

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

### Table 1. Single versus two-server topology

<table>
<thead>
<tr>
<th>One-server topology</th>
<th>Two-server topology</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Less computing power needed</td>
<td>• More processing power can be assigned to resource-hungry database queries.</td>
</tr>
<tr>
<td>• Faster installation</td>
<td>• Existing DB2 installation can be reused.</td>
</tr>
<tr>
<td></td>
<td>• Fast network connection to the database server is needed.</td>
</tr>
</tbody>
</table>

Note: If you choose to install Tivoli Asset Discovery for Distributed on the embedded WebSphere Application Server, you can later upgrade it to base WebSphere Application Server. No data is lost during the upgrade.

3. Choose the appropriate installation path:

   • Chapter 2, “Installing on embedded WebSphere Application Server,” on page 3
   • Installing on base WebSphere Application Server

### Supported operating systems for the server and database

Ensure that the computer where you are installing the IBM Tivoli Asset Discovery for Distributed server runs on one of the supported versions of operating systems.
Supported versions of IBM AIX®

<table>
<thead>
<tr>
<th>Version</th>
<th>Required level, service packs, patches</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.1</td>
<td></td>
</tr>
</tbody>
</table>
| 6.1     | • APAR IZ37466 - to apply the fix, the AIX® 6.1 instance must be upgraded to Technology Level 3.  
         • When installing the DB2 database on AIX, you also need the xIC.aix*.rte 8.0.0.4 or higher XL C/C++ runtime environment which you can download from [http://www-01.ibm.com/software/awdtools/xlcpp/support/](http://www-01.ibm.com/software/awdtools/xlcpp/support/).  
         • APAR IZ71102 - to apply the fix, the 6.1.3.6 libc library is required |
| 5.3 (64-bit) |                                        |

Supported versions of HP-UX

<table>
<thead>
<tr>
<th>Version</th>
<th>Required level, service packs, patches</th>
</tr>
</thead>
<tbody>
<tr>
<td>HP-UX 11i Integrity V11.23 Itanium (64-bit)</td>
<td></td>
</tr>
<tr>
<td>HP-UX 11i v3 Itanium (64-bit)</td>
<td></td>
</tr>
</tbody>
</table>

Supported versions of Red Hat Enterprise Linux

Note: In addition to the required packages listed below, you also must install the Compatibility Architecture Support or Compatibility Architecture Development Support on your system.

Table 3. Supported versions of Red Hat Enterprise Linux

<table>
<thead>
<tr>
<th>Version</th>
<th>Required level, service packs, patches</th>
</tr>
</thead>
<tbody>
<tr>
<td>6 for EM64T and AMD64 (64-bit)</td>
<td>compat-libstdc++-33 (32 and 64-bit)</td>
</tr>
</tbody>
</table>
| 6 for IBM Power Systems™ (64-bit) | compat-libstdc++-33 (32 and 64-bit)  
                                     | compat-libstdc++-295 (32 and 64-bit)  
                                     | Both 64-bit and 32-bit versions of the following packages:  
                                     | compat-db  
                                     | xorg-x11-deprecated-libs-6.8.1 or xorg-x11-deprecated-libs-6.8.2  
                                     | The following 32-bit version packages:  
                                     | pam  
                                     | cracklib-dicts  
                                     | cracklib  
                                     | glib2  
                                     | libselinux  
<pre><code>                                 | Update 1 or later for LPAR mobility |
</code></pre>
<table>
<thead>
<tr>
<th>Version</th>
<th>Required level, service packs, patches</th>
</tr>
</thead>
</table>
| 6 for IBM System z® (64–bit) | compat-libstdc++-295 (32 and 64-bit)  
Both 64-bit and 31-bit versions of the following packages:  
compat-db  
xorg-x11-deprecated-libs-6.8.1 or xorg-x11-deprecated-libs-6.8.2  
The following 31-bit version packages:  
pam  
cracklib-dicts  
cracklib  
glib2  
libselinux |
| 5 for EM64T and AMD64 (64–bit) | compat-libstdc++-33 (32 and 64-bit)  
Both 64-bit and 32-bit versions of the following packages:  
compat-db  
libXp  
The following 32-bit version packages:  
pam  
cracklib-dicts  
cracklib  
glib2  
libselinux |
| 5 for IBM Power Systems (64-bit) | compat-libstdc++-33 (32 and 64-bit)  
compat-libstdc++-295 (32 and 64-bit)  
Both 64-bit and 32-bit versions of the following packages:  
compat-db  
xorg-x11-deprecated-libs-6.8.1 or xorg-x11-deprecated-libs-6.8.2  
The following 32-bit version packages:  
pam  
cracklib-dicts  
cracklib  
glib2  
libselinux  
Update 1 or later for LPAR mobility |
| 5 for IBM System z (64–bit) | Update 1, compat-libstdc++-33 (32 and 64-bit)  
compat-libstdc++-295 (32 and 64-bit)  
Both 64-bit and 31-bit versions of the following packages:  
compat-db  
xorg-x11-deprecated-libs-6.8.1 or xorg-x11-deprecated-libs-6.8.2  
The following 31-bit version packages:  
pam  
cracklib-dicts  
cracklib  
glib2  
libselinux |
Supported versions of SUSE Linux Enterprise Server

<table>
<thead>
<tr>
<th>Version</th>
<th>Required level, service packs, patches</th>
</tr>
</thead>
<tbody>
<tr>
<td>11 for Intel/AMD x86</td>
<td></td>
</tr>
<tr>
<td>11 for EM64T and AMD64</td>
<td>pam-modules-32bit</td>
</tr>
<tr>
<td>11 for IBM Power Systems (64-bit)</td>
<td>pam-modules-32bit</td>
</tr>
<tr>
<td>11 for IBM System z (64-bit) on 64-bit hardware</td>
<td>pam-modules-32bit</td>
</tr>
<tr>
<td>10 for EM64T and AMD64</td>
<td>compat-libstdc++ (32 and 64-bit)</td>
</tr>
<tr>
<td></td>
<td>If you plan to install DB2 9.7:</td>
</tr>
<tr>
<td></td>
<td>Service Pack 2</td>
</tr>
<tr>
<td></td>
<td>glibc-2.4-31</td>
</tr>
<tr>
<td></td>
<td>libaio-64bit-0.3.104-14.2</td>
</tr>
<tr>
<td></td>
<td>The following 32-bit version packages:</td>
</tr>
<tr>
<td></td>
<td>pam</td>
</tr>
<tr>
<td></td>
<td>cracklib-dicts</td>
</tr>
<tr>
<td></td>
<td>cracklib</td>
</tr>
<tr>
<td></td>
<td>glib2</td>
</tr>
<tr>
<td></td>
<td>libselinux</td>
</tr>
<tr>
<td></td>
<td>The following 64-bit version packages:</td>
</tr>
<tr>
<td></td>
<td>xorg-x11-libs-64bit-6.9.0-50.58,ppc.rpm</td>
</tr>
<tr>
<td></td>
<td>expat-64bit-2.0.0-13.2,ppc.rpm</td>
</tr>
<tr>
<td></td>
<td>fontconfig-64bit-2.3.94-18.16,ppc.rpm</td>
</tr>
<tr>
<td></td>
<td>freetype2-64bit-2.1.10-18.14,ppc.rpm</td>
</tr>
<tr>
<td></td>
<td>pam-modules-32bit</td>
</tr>
<tr>
<td>Version</td>
<td>Required level, service packs, patches</td>
</tr>
<tr>
<td>---------</td>
<td>----------------------------------------</td>
</tr>
<tr>
<td>10 for IBM Power Systems (64-bit)</td>
<td>compat-libstdc++ (32 and 64-bit)</td>
</tr>
<tr>
<td></td>
<td>Service Pack 1 or later for LPAR mobility</td>
</tr>
<tr>
<td></td>
<td>If you plan to install DB2 9.7:</td>
</tr>
<tr>
<td></td>
<td>Service Pack 2</td>
</tr>
<tr>
<td></td>
<td>glibc-2.4-31</td>
</tr>
<tr>
<td></td>
<td>libaio-64bit-0.3.104-14.2</td>
</tr>
<tr>
<td></td>
<td>vacpp.rte-9.0.0-5</td>
</tr>
<tr>
<td></td>
<td>xlsmp.msg.rte-1.7.0-5</td>
</tr>
<tr>
<td></td>
<td>xlsmp.rte-1.7.0-5</td>
</tr>
<tr>
<td></td>
<td>The following 32-bit version packages:</td>
</tr>
<tr>
<td></td>
<td>pam</td>
</tr>
<tr>
<td></td>
<td>cracklib-dicts</td>
</tr>
<tr>
<td></td>
<td>cracklib</td>
</tr>
<tr>
<td></td>
<td>glib2</td>
</tr>
<tr>
<td></td>
<td>libselinux</td>
</tr>
<tr>
<td></td>
<td>The following 64-bit version packages:</td>
</tr>
<tr>
<td></td>
<td>xorg-x11-libs-64bit-6.9.0-50.58.ppc.rpm</td>
</tr>
<tr>
<td></td>
<td>expat-64bit-2.0.0-13.2.ppc.rpm</td>
</tr>
<tr>
<td></td>
<td>fontconfig-64bit-2.3.94-18.16.ppc.rpm</td>
</tr>
<tr>
<td></td>
<td>freetype2-64bit-2.1.10-18.14.ppc.rpm</td>
</tr>
<tr>
<td>10 for IBM System z (64-bit) on 64-bit hardware</td>
<td>compat-libstdc++ (32 and 64-bit)</td>
</tr>
<tr>
<td></td>
<td>If you plan to install DB2 9.7:</td>
</tr>
<tr>
<td></td>
<td>Service Pack 2</td>
</tr>
<tr>
<td></td>
<td>glibc-2.4-31</td>
</tr>
<tr>
<td></td>
<td>libaio-64bit-0.3.104-14.2</td>
</tr>
<tr>
<td></td>
<td>vacpp.rte-9.0.0-5</td>
</tr>
<tr>
<td></td>
<td>The following 31-bit version packages:</td>
</tr>
<tr>
<td></td>
<td>pam</td>
</tr>
<tr>
<td></td>
<td>cracklib-dicts</td>
</tr>
<tr>
<td></td>
<td>cracklib</td>
</tr>
<tr>
<td></td>
<td>glib2</td>
</tr>
<tr>
<td></td>
<td>libselinux</td>
</tr>
<tr>
<td></td>
<td>The following 64-bit version packages:</td>
</tr>
<tr>
<td></td>
<td>xorg-x11-libs-64bit-6.9.0-50.58.ppc.rpm</td>
</tr>
<tr>
<td></td>
<td>expat-64bit-2.0.0-13.2.ppc.rpm</td>
</tr>
<tr>
<td></td>
<td>fontconfig-64bit-2.3.94-18.16.ppc.rpm</td>
</tr>
<tr>
<td></td>
<td>freetype2-64bit-2.1.10-18.14.ppc.rpm</td>
</tr>
</tbody>
</table>

**Supported versions of Sun Solaris**
<table>
<thead>
<tr>
<th>Version</th>
<th>Operating System for SPARC platforms (64-bit)</th>
</tr>
</thead>
<tbody>
<tr>
<td>9</td>
<td>Operating System for SPARC platforms (64-bit)</td>
</tr>
</tbody>
</table>

### Supported versions of Windows

<table>
<thead>
<tr>
<th>Version</th>
<th>Required level, service packs, patches</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server 2008 R2 Datacenter</td>
<td></td>
</tr>
<tr>
<td>Server 2008 R2 Standard Edition (64-bit) for Intel x86</td>
<td></td>
</tr>
<tr>
<td>Server 2008 R2 Enterprise Edition (64-bit) for Intel x86</td>
<td></td>
</tr>
<tr>
<td>Server 2008 Standard Edition (32-bit and 64-bit) for Intel x86</td>
<td></td>
</tr>
<tr>
<td>Server 2008 Enterprise Edition (32-bit and 64-bit) for Intel x86</td>
<td></td>
</tr>
<tr>
<td>Server 2003 Enterprise Edition (32-bit and 64-bit)</td>
<td></td>
</tr>
</tbody>
</table>

### Supported partitioning technologies - servers

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

### CPU and memory requirements for the server and database

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

The requirements are divided into:

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

#### CPU requirements for environments with up to 5,000 agents

<table>
<thead>
<tr>
<th>Server</th>
<th>Required level, service packs, patches</th>
</tr>
</thead>
<tbody>
<tr>
<td>AIX and Linux</td>
<td>2 Power4 1.2 GHz</td>
</tr>
<tr>
<td>Linux and Windows x86, 32 and 64-bit</td>
<td>at least one Intel Core Solo T1300 1.66 GHz processor</td>
</tr>
<tr>
<td>Solaris SPARC</td>
<td>Sun-Fire-280R 1015 MHz two-way processor</td>
</tr>
<tr>
<td>HP-UX</td>
<td>rp2470, at least two PA-RISC 2.0 650 MHz processors</td>
</tr>
<tr>
<td>Linux on zSeries</td>
<td>Type 2084, one dedicated processor.</td>
</tr>
</tbody>
</table>
CPU requirements for environments with up to 5,000 agents


Memory requirements for environments with up to 5,000 agents

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Server only</td>
<td>1 GB RAM</td>
</tr>
<tr>
<td>Server and database</td>
<td>3 GB RAM</td>
</tr>
</tbody>
</table>

CPU requirements for environments with 5,000 to 45,000 agents

<table>
<thead>
<tr>
<th>Server</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>AIX and Linux</td>
<td>At least one Power6 4.7 GHz processor</td>
</tr>
<tr>
<td>Linux x86, 32 and 64–bit</td>
<td>Intel Xeon 2.5 GHz, four-way processor</td>
</tr>
<tr>
<td>Solaris SPARC</td>
<td>One SPARC VI, 2150 MHz (4 threads) processor</td>
</tr>
<tr>
<td>HP-UX</td>
<td>rp8420, at least two PA-RISC 2.0 1.0 GHz processors</td>
</tr>
<tr>
<td>Linux on zSeries</td>
<td>Type 2084, two dedicated processors</td>
</tr>
<tr>
<td>Windows x86, 32 and 64–bit</td>
<td>One Dual Core AMD Opteron, 2.6 GHz processor</td>
</tr>
</tbody>
</table>


Memory requirements for environments with 5,000 to 45,000 agents

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Server only</td>
<td>1 GB RAM</td>
</tr>
<tr>
<td>Server and database</td>
<td>4 GB RAM</td>
</tr>
</tbody>
</table>

**Space requirements for the server and database**

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

You can install the IBM Tivoli Asset Discovery for Distributed server and database on the same computer, or on two different computers. You need to install the DB2 database software before you start the installation process or you can use a working installation of DB2.

The table below shows how much space you need depending on your operating system and the components that you are installing on this machine. The space requirements for the server component were measured for the embedded version of WebSphere Application Server included in the installation package. If you want to install the Tivoli Asset Discovery for Distributed server on base WebSphere Application Server (recommended for large environments with more than 5000 agents), visit WebSphere Application Server information center for space requirements: [http://publib.boulder.ibm.com/infocenter/wasinfo/v7r0/index.jsp?topic=/com.ibm.websphere.nd.doc/info/welcome_nd.html](http://publib.boulder.ibm.com/infocenter/wasinfo/v7r0/index.jsp?topic=/com.ibm.websphere.nd.doc/info/welcome_nd.html)

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

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

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

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

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

The requirements below are for installation only.

<table>
<thead>
<tr>
<th>Operating system</th>
<th>Installed components</th>
<th>Directory</th>
<th>Required space</th>
</tr>
</thead>
<tbody>
<tr>
<td>AIX</td>
<td>Server and database (without the DB2 prerequisite)</td>
<td>Product installation directory</td>
<td>1941 MB</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Database installation directory</td>
<td>690 MB</td>
</tr>
<tr>
<td></td>
<td></td>
<td><code>/tmp</code></td>
<td>939 MB</td>
</tr>
<tr>
<td></td>
<td></td>
<td><code>/etc</code></td>
<td>under 1 MB</td>
</tr>
<tr>
<td></td>
<td></td>
<td><code>/var</code></td>
<td>260 MB</td>
</tr>
<tr>
<td></td>
<td>Total</td>
<td></td>
<td><strong>3831 MB</strong></td>
</tr>
<tr>
<td></td>
<td>Server only</td>
<td>Product installation directory</td>
<td>1941 MB</td>
</tr>
<tr>
<td></td>
<td></td>
<td><code>/tmp</code></td>
<td>939 MB</td>
</tr>
<tr>
<td></td>
<td></td>
<td><code>/etc</code></td>
<td>under 1 MB</td>
</tr>
<tr>
<td></td>
<td></td>
<td><code>/var</code></td>
<td>under 1 MB</td>
</tr>
<tr>
<td></td>
<td>Total</td>
<td></td>
<td><strong>2882 MB</strong></td>
</tr>
<tr>
<td></td>
<td>Database (without the DB2 prerequisite)</td>
<td>Product installation directory</td>
<td>239 MB</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Database installation directory</td>
<td>687 MB</td>
</tr>
<tr>
<td></td>
<td></td>
<td><code>/tmp</code></td>
<td>345 MB</td>
</tr>
<tr>
<td></td>
<td></td>
<td><code>/etc</code></td>
<td>under 1 MB</td>
</tr>
<tr>
<td></td>
<td></td>
<td><code>/var</code></td>
<td>125 MB</td>
</tr>
<tr>
<td></td>
<td>Total</td>
<td></td>
<td><strong>1397 MB</strong></td>
</tr>
<tr>
<td>Operating system</td>
<td>Installed components</td>
<td>Directory</td>
<td>Required space</td>
</tr>
<tr>
<td>------------------</td>
<td>--------------------------------------------</td>
<td>----------------------------</td>
<td>----------------</td>
</tr>
<tr>
<td>HP-UX</td>
<td>Server and database (without the DB2 prerequisite)</td>
<td>Product installation directory</td>
<td>1870 MB</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Database installation directory</td>
<td>593 MB</td>
</tr>
<tr>
<td></td>
<td></td>
<td>/tmp</td>
<td>473 MB</td>
</tr>
<tr>
<td></td>
<td></td>
<td>/etc</td>
<td>under 1 MB</td>
</tr>
<tr>
<td></td>
<td></td>
<td>/var</td>
<td>643 MB</td>
</tr>
<tr>
<td></td>
<td></td>
<td>/var/tmp</td>
<td>642 MB</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Total</td>
<td>4222 MB</td>
</tr>
<tr>
<td></td>
<td>Server only</td>
<td>Product installation directory</td>
<td>1845 MB</td>
</tr>
<tr>
<td></td>
<td></td>
<td>/tmp</td>
<td>470 MB</td>
</tr>
<tr>
<td></td>
<td></td>
<td>/etc</td>
<td>under 1 MB</td>
</tr>
<tr>
<td></td>
<td></td>
<td>/var/tmp</td>
<td>627 MB</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Total</td>
<td>2943 MB</td>
</tr>
<tr>
<td></td>
<td>Database (without the DB2 prerequisite)</td>
<td>Product installation directory</td>
<td>299 MB</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Database installation directory</td>
<td>595 MB</td>
</tr>
<tr>
<td></td>
<td></td>
<td>/tmp</td>
<td>502 MB</td>
</tr>
<tr>
<td></td>
<td></td>
<td>/etc</td>
<td>under 1 MB</td>
</tr>
<tr>
<td></td>
<td></td>
<td>/var</td>
<td>2 MB</td>
</tr>
<tr>
<td></td>
<td></td>
<td>/var/tmp</td>
<td>under 1 MB</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Total</td>
<td>1400 MB</td>
</tr>
<tr>
<td>Linux</td>
<td>Server and database (without the DB2 prerequisite)</td>
<td>Product installation directory</td>
<td>1889 MB</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Database installation directory</td>
<td>614 MB</td>
</tr>
<tr>
<td></td>
<td></td>
<td>/tmp</td>
<td>814 MB</td>
</tr>
<tr>
<td></td>
<td></td>
<td>/etc</td>
<td>under 1 MB</td>
</tr>
<tr>
<td></td>
<td></td>
<td>/var</td>
<td>2 MB</td>
</tr>
<tr>
<td></td>
<td></td>
<td>/var/tmp</td>
<td>under 1 MB</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Total</td>
<td>3321 MB</td>
</tr>
<tr>
<td></td>
<td>Server only</td>
<td>Product installation directory</td>
<td>1860 MB</td>
</tr>
<tr>
<td></td>
<td></td>
<td>/tmp</td>
<td>849 MB</td>
</tr>
<tr>
<td></td>
<td></td>
<td>/etc</td>
<td>under 1 MB</td>
</tr>
<tr>
<td></td>
<td></td>
<td>/var</td>
<td>4 MB</td>
</tr>
<tr>
<td></td>
<td></td>
<td>/var/tmp</td>
<td>under 1 MB</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Total</td>
<td>2715 MB</td>
</tr>
<tr>
<td></td>
<td>Database (without the DB2 prerequisite)</td>
<td>Product installation directory</td>
<td>296 MB</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Database installation directory</td>
<td>509 MB</td>
</tr>
<tr>
<td></td>
<td></td>
<td>/tmp</td>
<td>251 MB</td>
</tr>
<tr>
<td></td>
<td></td>
<td>/etc</td>
<td>under 1 MB</td>
</tr>
<tr>
<td></td>
<td></td>
<td>/var</td>
<td>2 MB</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Total</td>
<td>1059 MB</td>
</tr>
<tr>
<td>Operating system</td>
<td>Installed components</td>
<td>Directory</td>
<td>Required space</td>
</tr>
<tr>
<td>------------------</td>
<td>----------------------</td>
<td>-----------</td>
<td>----------------</td>
</tr>
<tr>
<td>Solaris</td>
<td>Server and database (without the DB2 prerequisite)</td>
<td>Product installation directory</td>
<td>1999 MB</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Database installation directory</td>
<td>650 MB</td>
</tr>
<tr>
<td></td>
<td></td>
<td>/tmp</td>
<td>441 MB</td>
</tr>
<tr>
<td></td>
<td></td>
<td>/etc</td>
<td>under 1 MB</td>
</tr>
<tr>
<td></td>
<td></td>
<td>/var</td>
<td>222 MB</td>
</tr>
<tr>
<td></td>
<td></td>
<td>/var/tmp</td>
<td>583 MB</td>
</tr>
<tr>
<td></td>
<td>Total</td>
<td></td>
<td>3896 MB</td>
</tr>
<tr>
<td>Server only</td>
<td></td>
<td>Product installation directory</td>
<td>1971 MB</td>
</tr>
<tr>
<td></td>
<td></td>
<td>/tmp</td>
<td>441 MB</td>
</tr>
<tr>
<td></td>
<td></td>
<td>/var</td>
<td>259 MB</td>
</tr>
<tr>
<td></td>
<td></td>
<td>/var/tmp</td>
<td>581 MB</td>
</tr>
<tr>
<td></td>
<td>Total</td>
<td></td>
<td>3252 MB</td>
</tr>
<tr>
<td>Database without the DB2 prerequisite</td>
<td></td>
<td>Product installation directory</td>
<td>263 MB</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Database installation directory</td>
<td>650 MB</td>
</tr>
<tr>
<td></td>
<td></td>
<td>/tmp</td>
<td>442 MB</td>
</tr>
<tr>
<td></td>
<td></td>
<td>/etc</td>
<td>under 1 MB</td>
</tr>
<tr>
<td></td>
<td></td>
<td>/var</td>
<td>under 1 MB</td>
</tr>
<tr>
<td></td>
<td></td>
<td>/var/tmp</td>
<td>under 1 MB</td>
</tr>
<tr>
<td></td>
<td>Total</td>
<td></td>
<td>1358 MB</td>
</tr>
<tr>
<td>Windows</td>
<td>Server and database (without the DB2 prerequisite)</td>
<td>Product installation directory</td>
<td>1881 MB</td>
</tr>
<tr>
<td></td>
<td></td>
<td>%TEMP%</td>
<td>739 MB</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Database installation directory</td>
<td>649 MB</td>
</tr>
<tr>
<td></td>
<td>Total</td>
<td></td>
<td>3269 MB</td>
</tr>
<tr>
<td>Server only</td>
<td></td>
<td>Product installation directory</td>
<td>1881 MB</td>
</tr>
<tr>
<td></td>
<td></td>
<td>%TEMP%</td>
<td>590 MB</td>
</tr>
<tr>
<td></td>
<td>Total</td>
<td></td>
<td>2471 MB</td>
</tr>
<tr>
<td>Database (without the DB2 prerequisite)</td>
<td></td>
<td>Product installation directory</td>
<td>234 MB</td>
</tr>
<tr>
<td></td>
<td></td>
<td>%TEMP%</td>
<td>198 MB</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Database installation directory</td>
<td>613 MB</td>
</tr>
<tr>
<td></td>
<td>Total</td>
<td></td>
<td>1045 MB</td>
</tr>
</tbody>
</table>

**Other software prerequisites**

Ensure that all required prerequisite software is installed on the computer where you are installing the IBM Tivoli Asset Discovery for Distributed server.

**Administration server**

*Table 4. Prerequisites for administration server*

| Database driver | JDBC driver type 4 is automatically installed if not already present. |
Table 4. Prerequisites for administration server (continued)

| UNIX shell | To install the server on UNIX platforms you must have the Bourne shell (sh) installed and activated. It is not necessary to run the installation from the Bourne shell. You also need to install and activate the Korn shell. |
| Web browser | A web browser is required to access the web user interface of the server. It is also needed for the installation launchpad to start; however, it is also possible to start the installation of Tivoli Asset Discovery for Distributed without the launchpad. Supported browsers on different platforms:  
  - Supported MS Windows versions  
    - Internet Explorer 6.x, and 7.x,  
    - Firefox 2.0.x  
  - Other supported platforms  
    - Firefox 2.0.x, 3.x  
  Note: It is important not to turn the JavaScript option off in the browser as some of the functionalities of the web interface might not function properly. For secure connections, cookies need to be enabled. |
| Gzip compression utility | UNIX Linux |
| gdiplus.dll library | Windows |

Gzip compression utility | UNIX Linux  
It is needed for the installation process to run.

gdiplus.dll library | Windows  
This library is needed to run the Tivoli Asset Discovery for Distributed Launchpad.

Administration server database

You have two options for installing the DB2 software prerequisite:
- You can install it ahead of time, using the installation media provided with Tivoli Asset Discovery for Distributed.
- You can use an existing instance of DB2 that you have already installed. Refer to the following table for required software levels.

Table 5. Prerequisites for administration server database

| Database server | DB2, Enterprise Server Edition server, version 9.7  
  - Fix Pack 2 to Fix Pack 9 (upon availability) - GA  
  - Fix Pack 6 and higher - [Fix Pack 2]  
| DB2, Enterprise Server Edition server, version 9.5  
  - Fix Pack 3 to Fix Pack 9 - GA  
  - Fix Pack 10 and higher - [Fix Pack 2]  
| DB2, Enterprise Server Edition server, version 9.1  
  - Fix Pack 7 to Fix Pack 9 - GA  
  - Fix Pack 12 and higher - [Fix Pack 2]  

Note:
1. The DB2 server must be configured for remote communication - the \texttt{svccname} parameter must be set.
2. DB2 9.1 is not supported on Windows Server 2008 R2.
3. If you want to apply Fix Pack 9 to DB2 version 9.1 and use it with the General Availability versions of Tivoli Asset Discovery for Distributed, first install Tivoli Asset Discovery for Distributed and then apply the fix pack. Alternatively, you can upgrade DB2 to version 9.5.
Table 5. Prerequisites for administration server database (continued)

<table>
<thead>
<tr>
<th>UNIX shell</th>
<th>To install the databases on UNIX platforms you must have the Korn shell (ksh) installed and activated. It must be set as the default shell for the DB2 instance owner. <strong>Note:</strong> The shell must be present but the setup command to install the database can be issued from any shell – not necessarily the Korn shell.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gzip compression utility</td>
<td>It is needed for the installation process to run.</td>
</tr>
</tbody>
</table>

**WebSphere Application Server**

You have two options for installing the WebSphere software prerequisite:

- If you do not plan to support more than 5000 agents, you can install the *embedded* version of the WebSphere Application Server from the Tivoli Asset Discovery for Distributed wizard.

- To support a larger infrastructure, you must install a base version of WebSphere Application Server before installing Tivoli Asset Discovery for Distributed. You can install the base edition using the 6.1 installation media that are provided with this product, or you can use an existing installation of WebSphere Application Server 6.1. You must install Fix Pack 33 or later for the product to function properly. For more details about WebSphere installation, refer to the WebSphere information center.

Table 6. Prerequisites for WebSphere Application Server

<table>
<thead>
<tr>
<th>Preparing the operating system for product installation</th>
<th>Preparing the operating system for product installation</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>embedded</strong> WebSphere Application Server 6.1</td>
<td>This fix pack and Update Installer are shipped with the product.</td>
</tr>
<tr>
<td>Fix Pack 33</td>
<td></td>
</tr>
<tr>
<td><strong>base</strong> WebSphere Application Server 6.1</td>
<td>Fix list for IBM WebSphere Application Server V6.1</td>
</tr>
<tr>
<td>Fix Pack 33</td>
<td></td>
</tr>
</tbody>
</table>

**IBM Software Knowledge Base Toolkit 1.2 (required)**

Software Knowledge Base Toolkit helps you with maintaining an up-to-date repository of knowledge about software products and the means to discover them as installed and running on computer systems. For hardware and software requirements, see: [Installation requirements for version 1.2](#). To download Software Knowledge Base Toolkit version 1.2, log in to the Passport Advantage website and search for the following part number: CI0HQML.

**Important:** Software Knowledge Base Toolkit version 1.2.2 is also supported by Tivoli Asset Discovery for Distributed. To upgrade to version 1.2.2, go to [fix central](#) and download an upgrade package that is suitable for the operating system on which you have Software Knowledge Base Toolkit installed.

- For software and hardware requirements as well as other relevant information, see the [product documentation](#).

- For information about interim fix 1 for version 1.2.2, see: [http://www-01.ibm.com/support/docview.wss?uid=swg24037002](http://www-01.ibm.com/support/docview.wss?uid=swg24037002)
IBM Tivoli Common Reporting 2.1 (optional)

For hardware and software requirements refer to the [product documentation](#).

Integration with IBM Tivoli Asset Management for IT and Tivoli Integration Composer (ITIC)

Tivoli Asset Discovery for Distributed exchanges data with the following software versions:

<table>
<thead>
<tr>
<th></th>
<th>Version</th>
<th>More information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tivoli Asset Management for IT</td>
<td>7.2.2</td>
<td><a href="#">Product documentation</a></td>
</tr>
<tr>
<td>Tivoli Integration Composer</td>
<td>7.2.2.1</td>
<td><a href="#">Product documentation</a></td>
</tr>
</tbody>
</table>

Supported versions of WebSphere Application Server

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

Tivoli Asset Discovery for Distributed supports the following versions of WebSphere:

- WebSphere Application Server, version 6.1 with at least Fix Pack 33
- WebSphere Application Server Network Deployment, version 6.1 (standard application server profile only) with at least Fix Pack 33

For more information about hardware and software requirements for the application, see [Preparing for product installation](#).

On Solaris 9 operating system for SPARC platforms (64-bit), Tivoli Asset Discovery for Distributed supports only the 32-bit version of the application server.

**Note:** If you are installing on the base version of WebSphere Application Server, with enabled secure agent-server communication, you must apply a Java™ update on WebSphere Application Server. You can download the update from the following page: [http://www-01.ibm.com/support/docview.wss?rs=180&uid=swg24019127](http://www-01.ibm.com/support/docview.wss?rs=180&uid=swg24019127). If you do not apply the Java update, the secure communication will not work properly. Depending on the security level, the agent will be able to connect to the server but other operations such as catalog download or the import of a private certificate when configuring agents will cause GSKit exceptions.

Topology and capacity planning

Before installing IBM Tivoli Asset Discovery for Distributed to monitor the installed software in your organization, you need to plan the placement of the product components.

Scan groups

Scan groups are units for grouping agents. Scans of installed software and hardware are scheduled on a scan group level. Decide how you want to divide agents between scan groups so that the operations which you can perform by scan groups are meaningful within your organization. Each agent must be assigned to a scan group.
Note: Creating scan groups is not mandatory but preferable. There is always a scan group to which agents are assigned by default.

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

**Placement of server components**

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

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

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

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

**Placement of agents**

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

**Agent backward compatibility**

The following versions of Tivoli Asset Discovery for Distributed agents are able to connect to the Tivoli Asset Discovery for Distributed 7.2.2 server:

- Tivoli Asset Discovery for Distributed 7.2.1 GA, and Fix Pack 1
- Tivoli Asset Discovery for Distributed 7.2 GA, and Fix Pack 1
- License Metric Tool 7.1 GA, and Fix Pack 1
- Tivoli License Compliance Manager 2.3 Fix Pack 5 or higher

**Using secure communications**

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

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

A single agent does not require high bandwidth for the communication with the server. The amount of data exchanged with the Tivoli Asset Discovery for Distributed server can be as high as 350 kilobytes in a 24-hour timeframe (This includes the upload of software and hardware scan results).

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

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

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

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

*Table 7. Ports used by Tivoli Asset Discovery for Distributed*

<table>
<thead>
<tr>
<th>Type</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Interface</td>
<td>8899 (http) and 8888 (https)</td>
</tr>
<tr>
<td></td>
<td>These ports are default ports for embedded WebSphere Application Server. If you are not using default ports, you can check the port values in Installation_folder/admin/master.tag. For the base version of WebSphere Application Server, the port numbers are characteristic of the profile on which the product is deployed.</td>
</tr>
<tr>
<td>Agent-server communication</td>
<td>9988 (http), 9999 (https) and 9977 (https with client authentication)</td>
</tr>
<tr>
<td>Database (DB2)</td>
<td>default value of 50000</td>
</tr>
</tbody>
</table>

Security considerations

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

Required access privileges for the installation

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

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

Local operating system registries

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

Levels of security

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

Minimum

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

Medium

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

Maximum

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

Ports

For the list of ports used by Tivoli Asset Discovery for Distributed, go to “Network planning” on page 18.

Security-Enhanced Linux

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

Proof-of-concept installation

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

Proof-of-concept installation has all the functions of the production version, but the database parameters are scaled down and the communication times between product components are reduced. If you use this mode of installation, you cannot install the administration server and administration server database on separate computers. You can launch proof-of-concept installation by selecting Test Environment at the start of the server installation.
**Note:** Proof-of-concept installation can be performed only on the embedded version of WebSphere Application Server.

After you finish testing, you should uninstall the *proof-of-concept* instance of the server, and install Tivoli Asset Discovery for Distributed server again in *production* mode. You can also uninstall only the administration server database leaving the administration server untouched, and then install the database in production mode. In both cases, all the server settings as well as the data already gathered by the agents will be lost. It is therefore important to consider this change early in the planning process.

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

*Table 8. Proof-of-concept and production installations*

<table>
<thead>
<tr>
<th>Configuration parameters stored in the database</th>
<th>Test (proof-of-concept) environment</th>
<th>Production environment</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Server</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>BUFFERPOOL</td>
<td>20000</td>
<td>80000</td>
</tr>
<tr>
<td>upload_usage_period (minutes)</td>
<td>5</td>
<td>360</td>
</tr>
<tr>
<td>ping_period (minutes)</td>
<td>2</td>
<td>60</td>
</tr>
<tr>
<td>report_finalization_delay (days)</td>
<td>1</td>
<td>7</td>
</tr>
<tr>
<td>testEnvironmentEnabled</td>
<td>true</td>
<td>false</td>
</tr>
<tr>
<td>fipsEnabled</td>
<td>false</td>
<td>false</td>
</tr>
<tr>
<td>agentToServerSecurityLevel</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>productInventoryBuilderPeriod (minutes)</td>
<td>60</td>
<td>300</td>
</tr>
<tr>
<td>maxAggregateUsageAge (days)</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>inventoryScanGracePeriod (hours)</td>
<td>1</td>
<td>10</td>
</tr>
<tr>
<td><strong>Agents</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>down_parms_period (minutes)</td>
<td>7</td>
<td>360</td>
</tr>
<tr>
<td>maxAgentInactivity (minutes)</td>
<td>30</td>
<td>10080</td>
</tr>
<tr>
<td>maxAgentInactivityToDelete (minutes)</td>
<td>43200</td>
<td>43200</td>
</tr>
</tbody>
</table>

**Capacity Planning and recommendations**

For any large-scale DBMS updates, it must be ensured that statistics are collected as soon as possible. The simplest method to collect statistics is to run the following DB2 command: `reorgchk update statistics on table all`.

Recommended machines for such configuration can include:
- IBM System xSeries 335
- IBM System xSeries 336
- IBM System xSeries 3650

The general disk configuration requirements are:
- WebSphere Application Server: 50 GB
- DB2 server: 150 GB

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

Table 9. Suggested hardware requirements for two-server configurations

<table>
<thead>
<tr>
<th>Product component</th>
<th>1-10 products</th>
<th>11-35 products</th>
<th>36-50 products</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fewer than 5000 agents</td>
<td>WebSphere Application Server</td>
<td>1 core, 2 GB</td>
<td>1 core, 2 GB</td>
</tr>
<tr>
<td></td>
<td>DB2</td>
<td>1 core, 2 GB</td>
<td>1 core, 2 GB</td>
</tr>
<tr>
<td>5000 - 50000 agents</td>
<td>WebSphere Application Server</td>
<td>2 cores, 2 GB</td>
<td>2 cores, 2 GB</td>
</tr>
<tr>
<td></td>
<td>DB2</td>
<td>2 cores, 3 GB</td>
<td>2 cores, 3 GB</td>
</tr>
</tbody>
</table>

Tuning recommendations

The following properties are recommended:

Table 10. WebSphere Application Server parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Java Virtual Machine Heap</td>
<td>256 initial, 1024 maximum</td>
</tr>
<tr>
<td>Default Thread Pool</td>
<td>maximum size: 100</td>
</tr>
<tr>
<td>Message Handler Thread Pool</td>
<td>50 maximum: 50</td>
</tr>
<tr>
<td>Web Container Thread Pool</td>
<td>maximum size: 250</td>
</tr>
<tr>
<td>License Metric Tool Connection pools</td>
<td>maximum connections 10</td>
</tr>
<tr>
<td>LMTHW Connection pools</td>
<td>maximum connections 10</td>
</tr>
<tr>
<td>Connection pools for Message Handler Data Source</td>
<td>maximum connections 101 (2 X Threads +1) (for &gt;25000 agents@50 products)</td>
</tr>
</tbody>
</table>

Table 11. DB2 parameters

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Logfilesize</td>
<td>5000 (for more than 25000 agents, 50 products)</td>
</tr>
<tr>
<td>Logprimary</td>
<td>120</td>
</tr>
<tr>
<td>Logsecond</td>
<td>80</td>
</tr>
</tbody>
</table>

Increasing the size of the transaction log for greater than 25000 agents at 50 products per agent prevents the transaction log from being filled. If the transaction log is full, the aggregation does not run. Trace.logs will contain `<Exception><![CDATA[com.ibm.db2.jcc.b.SqlException: The transaction log for the database is full.]]>`

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

log ;-------Start of DE processing------- = [10/18/09 16:56:04:482 EDT], key = com.ibm.websphere.ce.j2c.ConnectionWaitTimeoutException Max connections reached
Note: It may also be possible to avoid max connection by increasing timeout period.

7.2.1 and 7.2.2 on 64-bit Linux test environment

Compare possibilities of IBM Tivoli Asset Discovery for Distributed versions 7.2.1 and 7.2.2 test on 64-bit Linux environment.

Elapsed time for Inventory Builder process is taken from trace.log files. Tivoli Asset Discovery for Distributed version 7.2.2 has significant improvements in the Inventory Builder processing time.

**Inventory Builder process**
50 products per agent, Linux 64 TAD4D server

![Graph showing Inventory Builder process time for 7.2.1 and 7.2.2](image)

Elapsed time for Aggregation increased for Tivoli Asset Discovery for Distributed version 7.2.2.

**Aggregation**
50 products per agent, Linux 64 TAD4D server

![Graph showing Aggregation time for 7.2.1 and 7.2.2](image)

The combined Inventory Builder and Aggregation times overall for Tivoli Asset Discovery for Distributed version 7.2.2 decreased compared to version 7.2.1.
Inventory Builder and Aggregation
50 products per agent, Linux 64 TAD4D Server

Tivoli Asset Discovery for Distributed version 7.2.2 DB2 size after Inventory Builder and Aggregation completed increased. In both test environments, 50 products per agent were configured.

Inventory Builder
TAD4D 7.2.2 Linux 64

Products per agent impact on Inventory Builder and Aggregation
Learn how number of installed agents influences Inventory Builder and Aggregation.

Aggregation is a process that runs daily and that processes data collected by agents to calculate PVU consumption and capacity for tier based systems software. The output of this process forms the basis for an audit report.

Inventory Builder is a process that assigns components to products, for example the existing installation of DB2 is matched with DB2 Enterprise Server Edition instead of DB2 Workgroup Server Edition.

Inventory Builder process time increases with the number of products per agent.
DB2 database size increases after Inventory Builder and Aggregation processes are completed.

**Inventory Builder and Aggregation**

50 products per agent - with usage, TAD4D7.2.1 vs. TAD4D7.2.2 Linux 64

Typically Total CPU is 30% busy during the entire interval. One day of aggregation configured. Tivoli Asset Discovery for Distributed version 7.2.2 CPU time starts to digress from the time reported by the trace logs after about 10000 agents. This post processing CPU activity can be eliminated by eliminating usage specification from the agents.
When using 10 products per agent, the elapsed CPU working time matches the total time reported by the trace logs.

**TAD4D 7.2.2 Linux 64**

25 products per agent - with usage

The difference between log times and actual CPU times starts to occur with more than 20000 agents with 25 products per agent.
The post processing CPU activity time increases with the number of products per agent increase and the total number of agents. This is due to a DB2 task that is deleting rows from usage_comp table per transaction. If usage is not specified, then the CPU activity matches the time specified in the logs for Inventory Builder and Aggregation.

**TAD4D 7.2.2 - Inventory Builder and Aggregation**

Linux 32 - 50 products per agent with usage

The same disparity between CPU activity time and time reported by the logs for Inventory Builder and Aggregation caused by usage, exists on Linux 32 platform.
**TAD4D 7.2.2**
1000 Agents

![Graph showing Elapsed time for Aggregation and Inventory Builder]

Configuring Tivoli Asset Discovery for Distributed or Tivoli License Metric Tool Server on same processor with same agent configuration resulted in similar times for the Inventory Builder process.

**4GB RAM - Inventory Builder process**
Solaris 2-way 1015Mhz processor

![Graph showing Elapsed time vs Number of agents]

**Recalculation**
Recalculation process is a linear operation depending on the number of agents and the number of days of aggregation.

Recalculation is a process that calculates new PVU consumption for all installed products in a given infrastructure after re-bundling has taken place (or after some products have been excluded, for example, in case of software beta testing).

For a large-scale environment with many days of aggregation recalculation process might involve many days of CPU consumption. In this case a 4-way processor was used and 25% CPU busy is equivalent to one processor running 100% busy.
Recalculation
200-1000 agents

Using actual times with a small scale environment, a multiplication factor was determined to calculate the amount of time that could be taken for recalculation process to complete in a large-scale environment. It is recommended to keep the number of days of aggregation to a minimum.

Table 12. Projections for recalculation time for large scale environment

<table>
<thead>
<tr>
<th>Agents</th>
<th>Days aggregated</th>
<th>Actual ET (m)</th>
<th>Mult factor</th>
<th>Total minutes</th>
<th>Total hours</th>
<th>Total days</th>
</tr>
</thead>
<tbody>
<tr>
<td>200</td>
<td>1</td>
<td>2</td>
<td>0.0083</td>
<td>1.66</td>
<td>0.03</td>
<td>0.00</td>
</tr>
<tr>
<td>200</td>
<td>10</td>
<td>19</td>
<td>0.0083</td>
<td>16.6</td>
<td>0.28</td>
<td>0.01</td>
</tr>
<tr>
<td>200</td>
<td>30</td>
<td>47</td>
<td>0.0083</td>
<td>49.8</td>
<td>0.83</td>
<td>0.03</td>
</tr>
<tr>
<td>1000</td>
<td>30</td>
<td>250</td>
<td>0.0083</td>
<td>249</td>
<td>4.15</td>
<td>0.17</td>
</tr>
<tr>
<td>5000</td>
<td>2</td>
<td>91</td>
<td>0.0083</td>
<td>83</td>
<td>1.38</td>
<td>0.06</td>
</tr>
<tr>
<td>45000</td>
<td>30</td>
<td></td>
<td>0.0083</td>
<td>11205</td>
<td>186.75</td>
<td>7.78</td>
</tr>
<tr>
<td>45000</td>
<td>90</td>
<td></td>
<td>0.0083</td>
<td>33615</td>
<td>560.25</td>
<td>23.34</td>
</tr>
</tbody>
</table>

DB size
Tivoli Asset Discovery for Distributed version 7.2.2 has on average about a 50% increase in DB size over version 7.2.1 depending on the scale of the configuration.
Table 13. DB size growth

<table>
<thead>
<tr>
<th>Number of agents</th>
<th>Tivoli Asset Discovery for Distributed 7.2.1 DB size (MB)</th>
<th>Tivoli Asset Discovery for Distributed 7.2.2 DB size (MB)</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>217.4</td>
<td>281.5</td>
</tr>
<tr>
<td>1</td>
<td>221.3</td>
<td>292.4</td>
</tr>
<tr>
<td>1000</td>
<td>252.6</td>
<td>356.2</td>
</tr>
<tr>
<td>5000</td>
<td>376.2</td>
<td>379.3</td>
</tr>
<tr>
<td>45000</td>
<td>1616 (p)</td>
<td>2875 (p)</td>
</tr>
<tr>
<td>slope</td>
<td>0.030986</td>
<td>0.057391</td>
</tr>
</tbody>
</table>

Chapter 2. Installing on embedded WebSphere Application Server
Table 14. DB size growth

<table>
<thead>
<tr>
<th>Number of agents</th>
<th>Tivoli Asset Discovery for Distributed 7.2.1 DB size (MB)</th>
<th>Tivoli Asset Discovery for Distributed 7.2.2 DB size (MB)</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>217.4</td>
<td>281.5</td>
</tr>
<tr>
<td>1</td>
<td>221.3</td>
<td>292.4</td>
</tr>
<tr>
<td>100</td>
<td>225.2</td>
<td>301.9</td>
</tr>
<tr>
<td>1000</td>
<td>277.1</td>
<td>390.4</td>
</tr>
<tr>
<td>5000</td>
<td>495.8</td>
<td>737.4</td>
</tr>
<tr>
<td>45000</td>
<td>2692 (p) 2705 (p)</td>
<td>4301 (p)</td>
</tr>
<tr>
<td>slope</td>
<td>0.054911</td>
<td>0.089018</td>
</tr>
</tbody>
</table>
Separate-server installation

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

Comparing Inventory Builder and Aggregation times, a 40% reduction in elapsed time when using a separate DB2 server. Both the Tivoli Asset Discovery for Distributed server and DB2 server were running on identical Linux 32-bit platforms. Linux 64-bit running on a 2.6 GHz processor was comparable to Linux 32-bit running on a 2.4 GHz processor. Most of the CPU time consumed is attributed to DB2 processes. Using the fastest processor available for DB2 would yield the most benefit in elapsed time for Inventory Builder and Aggregation processes.
Inventory Builder and Aggregation
Processor comparison - 50 products per agent - 1 day Aggregation

Sequence scenarios
WebUI response time of Home, PVU Current® Capacity, Software Products, Hardware, list agents activity without any other operation running. Each WebUI activity consumes 25% CPU busy on the 4-way Tivoli Asset Discovery for Distributed server.

Linux Server WebUI operations
Web UI response time of Home, PVU Current Capacity, Software Products, Hardware, list agents activity with Software Catalog import running. The software catalog import already consumes 25% CPU of the 4-way Tivoli Asset Discovery for Distributed server. The Web UI activities running on top of the SW catalog import increase total CPU consumed as well as, in some cases, add to response time for the Web UI operations to complete.
CPU activity of Software Catalog import along with varying amounts of agents and aggregation. Tivoli Asset Discovery for Distributed server running on a 4-way processor so 25% CPU is equivalent to one processor running 100% busy.

Installing the server (embedded WebSphere Application Server)

After you have decided on the installation path, check the software and hardware requirements. Then, install the server either on the embedded or base WebSphere Application Server.

Installation checklist - installing on embedded WebSphere Application Server (interactive and silent modes)

You can print the checklist and use it during the installation to ensure that you have completed all the necessary steps.
### Table 16. Installing Tivoli Asset Discovery for Distributed on the embedded version of WebSphere Application Server

<table>
<thead>
<tr>
<th>Step</th>
<th>Task</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>1 Plan and prepare to install</strong></td>
<td></td>
</tr>
<tr>
<td>1.1</td>
<td>Plan the topology.</td>
</tr>
<tr>
<td></td>
<td>Depending on your needs you can install the server with the embedded or base WebSphere Application Server. You can also consider installing DB2 on a separate server computer.</td>
</tr>
<tr>
<td>1.2</td>
<td>Ensure that the computer where you are installing the server fulfills all software and hardware requirements.</td>
</tr>
<tr>
<td></td>
<td>Before you install the server, you need to make sure that the computer meets the minimal CPU, and memory requirements for the server and database elements. You also need to check if there is enough disk space for the installation. Next, ensure that you use one of the supported operating systems and all the prerequisite software is installed.</td>
</tr>
<tr>
<td>1.3</td>
<td>Ensure that you have the required version of DB2 and its fix packs installed on your computer</td>
</tr>
<tr>
<td></td>
<td>The supported versions of DB2 are: 9.1, 9.5, and 9.7.</td>
</tr>
<tr>
<td>1.4</td>
<td>Consider the level of security for the communication between the server and agents.</td>
</tr>
<tr>
<td></td>
<td>You need to take into consideration the level of security that you want to use for the communication between the server and agents.</td>
</tr>
<tr>
<td><strong>2 Install the server</strong></td>
<td></td>
</tr>
<tr>
<td>2.1</td>
<td>Prepare the files for installation.</td>
</tr>
<tr>
<td></td>
<td>If you have downloaded the installation images from Passport Advantage, place them in a single directory on the computer where you are running the installer.</td>
</tr>
<tr>
<td>2.2</td>
<td>If you are installing the server and its database on different computers, synchronize the clocks of the server and database computers.</td>
</tr>
<tr>
<td></td>
<td>If you have decided to install the server and the database on separate computers, the time difference between the two computers should not be greater than 300 seconds.</td>
</tr>
<tr>
<td>2.3</td>
<td><strong>Linux</strong> Change SELinux settings.</td>
</tr>
<tr>
<td></td>
<td>To ensure proper server installation, you need to change the SELinux settings from enforcing mode to either permissive or disabled.</td>
</tr>
<tr>
<td>2.4</td>
<td>If you have decided to install the server in interactive mode, run the installation wizard.</td>
</tr>
<tr>
<td></td>
<td>In this option, you need to specify all parameters as the installation proceeds. If you have decided to install the database on a separate computer than the server, for example to improve the performance of the server, run the installer twice on each of the computers. DB2 software should already be installed on the designated computer.</td>
</tr>
<tr>
<td></td>
<td>As an alternative to using the installation wizard, you can specify parameters in a response file and start the installation from the command-line interface.</td>
</tr>
<tr>
<td>2.5</td>
<td>Verify the installation that you have run either in interactive or in silent mode.</td>
</tr>
<tr>
<td></td>
<td>To make sure that the installation has been successful, check the log files and start the Web user interface. Open the msg_servers.log file and check if it contains information that the application was successfully installed. The file is by default stored under the following path: Tivoli_Common_Directory/COOD/logs/install/message. Access the login page at the following address: http://administration_server_IP_address:8899/ibm/console/login.do and check the Home page for information about any problems that might have occurred during installation.</td>
</tr>
<tr>
<td>2.6</td>
<td><strong>Install IBM Software Knowledge Base Toolkit and then perform a few important postinstallation steps to configure Software Knowledge Base Toolkit to work with Tivoli Asset Discovery for Distributed.</strong></td>
</tr>
</tbody>
</table>
### Table 16. Installing Tivoli Asset Discovery for Distributed on the embedded version of WebSphere Application Server (continued)

<table>
<thead>
<tr>
<th>Step</th>
<th>Task</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.7</td>
<td>Install Tivoli Common Reporting if you would like to generate more accurate and detailed summary and trend reports.</td>
<td></td>
</tr>
</tbody>
</table>

### 3 Configure the administration server (information is available in a separate PDF file)

| 3.1  | Enable and configure the server security. |        |
|      | This is very important as the majority of the commands can only be run only after security has been enabled on the server. |        |
| 3.2  | Configure permissions for users |        |
|      | After you have enabled security for the Tivoli Asset Discovery for Distributed server, you need to configure access rights for the users. You can do it by assigning users to roles. |        |
| 3.3  | Configure Tivoli Asset Discovery for Distributed to work with Software Knowledge Base Toolkit. See Configuring IBM Tivoli Asset Discovery for Distributed 7.2.2 for more information. |        |
| 3.4  | Import the software catalog |        |
|      | The IBM® catalog is a knowledge base of product information that provides the information required by Tivoli Asset Discovery for Distributed to recognize which products are installed and in use on monitored computers. For more information see Configuring IBM Tivoli Asset Discovery for Distributed 7.2.2. |        |
| 3.5  | Import the processor value units table |        |
|      | Use the Integrated Solutions Console to obtain the processor value units table and import it into the database. See Configuring IBM Tivoli Asset Discovery for Distributed 7.2.2 for more information. |        |
| 3.6  | Import the most up-to-date systems tier table |        |
|      | Automatically download the most up-to-date systems tier table from IBM to account for new machines that have been manufactured and for new products that have been released. See Configuring IBM Tivoli Asset Discovery for Distributed 7.2.2 for more information. |        |
| 3.7  | Optional. Configure event notifications |        |
|      | You can configure the server to generate email notifications of significant licensing and system administration events. The notifications are then sent to recipients that you select in the Web interface. To configure event notifications, use the setserverconf command. For more information see Configuring IBM Tivoli Asset Discovery for Distributed 7.2.2. |        |

### Preinstallation steps

Before you start the installation, prepare installation images and install DB2. If you want to install the server and the database on different computers, synchronize the server and database clocks.

1. “Preparing installation images” on page 36
2. “Server installer files” on page 36
3. “A summary of Tivoli Asset Discovery for Distributed 7.2.2 installation images” on page 37
4. “Information regarding installing DB2” on page 38
5. “Synchronizing the clocks of server and database computers” on page 39
6. “Changing SELinux settings before installing Tivoli Asset Discovery for Distributed on Red Hat Linux” on page 39
Preparation of Installation Images

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

There are two forms of installation media:

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

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

Procedure

1. Download the software from Passport Advantage. Information about the download is described in the download document. Use the tabs to open the download documents for supported operating systems.
2. On the computer where you are running the installer, log on as root (UNIX or Linux) or Administrator (Windows).
3. Place all the downloaded installation images in a single directory on the computer where you are running the installer. For example:

   - **Linux**
     `/install_images`
   - **UNIX**
     `/install_images`
   - **Windows**
     `C:\install_images`

   **Note:** It is important to extract the files on the computer where you are running the installer, because the files must have the correct permissions when you extract them from the images.
4. Extract the contents of all installation images to the directory that you have created.

Server installer files

After you extract the installer file on a given platform, a directory structure is created with different installer files.

<table>
<thead>
<tr>
<th>Path (Windows platform)</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>\server\parts\CDROM_Installers\Disk1\InstData\Win32\VM\eWAS_6.1.0.23.zip</code></td>
<td>Embedded WebSphere Application Server package</td>
</tr>
<tr>
<td><code>\server\parts\CDROM_Installers\Disk1\InstData\platform\setupServers.exe</code> or <code>\server\parts\CDROM_Installers\Disk1\InstData\platform\setupServers.bin</code></td>
<td>Installation application launcher</td>
</tr>
<tr>
<td><code>\server\parts\CDROM_Installers\Disk1\InstData\Resource1.zip</code> and <code>\server\parts\CDROM_Installers\Disk1\InstData\MediaId.properties</code></td>
<td>Internal installer files</td>
</tr>
<tr>
<td><code>\server\parts\CDROM_Installers\Disk1\InstData\desc</code></td>
<td>Image description</td>
</tr>
<tr>
<td><code>\install\installResponsePOC.txt</code></td>
<td>The response file used in test installation</td>
</tr>
<tr>
<td><code>\install\installResponseProduction.txt</code></td>
<td>The response file used in production installation</td>
</tr>
</tbody>
</table>
Table 17. The most important Tivoli Asset Discovery for Distributed installer files (continued)

<table>
<thead>
<tr>
<th>Path (Windows platform)</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>\TAD4D-server-7.2.2-windows-x86_number_of_bits.bat or \TAD4D-server-7.2.2-operating_system-platform_number_of_bits.sh</td>
<td>The server installer file name (by platform)</td>
</tr>
<tr>
<td>\tools\expmap</td>
<td>The directory contains the ExpMapTool files. The ExpMapTool exports the deployment configuration of Tivoli License Compliance Manager 2.3 into an XML file.</td>
</tr>
<tr>
<td>\tools\checkVersion.sh</td>
<td>The script checks the version of WebSphere Application Server on UNIX and Linux operating systems. This script calls the checkVersion.jacl script.</td>
</tr>
<tr>
<td>\tools\checkVersion.jacl</td>
<td>The JACL script checks the version of WebSphere Application Server and Integrated Solutions Console.</td>
</tr>
<tr>
<td>\tools\checkVersion.bat</td>
<td>The script checks the version of WebSphere Application Server on Windows platform.</td>
</tr>
<tr>
<td>\tools\getarch</td>
<td>Internal installer helper script</td>
</tr>
<tr>
<td>\license\supported_lang_directory</td>
<td>The license directory contains sixteen sub-directories with IBM licenses in supported national languages.</td>
</tr>
<tr>
<td>\license\non_ibm_license.txt</td>
<td>The file contains terms and conditions for separately licensed code.</td>
</tr>
<tr>
<td>\license\notices.txt</td>
<td>The file contains notices and third party license terms and conditions.</td>
</tr>
<tr>
<td>\launchpad\</td>
<td>The directory contains launchpad binary, content and configuration files.</td>
</tr>
</tbody>
</table>

A summary of Tivoli Asset Discovery for Distributed 7.2.2 installation images

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

Table 18. Installation packages for installing on the embedded WebSphere Application Server

<table>
<thead>
<tr>
<th>No</th>
<th>Type of image</th>
<th>If you install on embedded WebSphere Application Server</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Server images</td>
<td>Tivoli Asset Discovery for Distributed 7.2.2 platform specific server installation package. It contains the following packages:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• The embedded WebSphere Application Server 6.1 is packaged with the Tivoli Asset Discovery for Distributed 7.2.2 server installation package</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Integrated Solutions Console version 7.1.0.9 package for embedded Websphere Application Server</td>
</tr>
</tbody>
</table>
Table 18. Installation packages for installing on the embedded WebSphere Application Server (continued)

<table>
<thead>
<tr>
<th>No</th>
<th>Type of image</th>
<th>If you install on embedded WebSphere Application Server</th>
</tr>
</thead>
</table>
| 2. | Agent images  | • Tivoli Asset Discovery for Distributed 7.2.2 agent installation package (native installer)  
|    |               | • Agent installation package, collection of Software Package Blocks only for Tivoli Configuration Manager-based installation  
|    |               | • Agent shell installation packages for all UNIX platforms  
|    |               | • Agent shell installation package, collection of all shell installers  
|    |               | • Common Inventory Technology Enabler |
| 3. | WebSphere Application Server images | IBM Update Installer 7.0.0.9 for WebSphere Software is available on the following download page or on the product DVD, in the directory server/fixpacks.  
|     |               | If you are installing on the embedded WebSphere Application Server, you do not need to install the fix packs - they are installed together with the application server (Fix packs for embedded WebSphere Application Server are shipped within the server installation package). |
| 4. | DB2 images    | • DB2 Enterprise Server Edition 9.7  
|     |               | • DB2 Enterprise Server Edition 9.7 Restricted Use Activation |
| 5. | Documentation images | • Quick Start Guide  
|     |               | • Tivoli Asset Discovery for Distributed 7.2.2 Quick Start (this image contains complete information center). |
| 6. | Additional images | • IBM Prerequisite Scanner for UNIX platforms  
|     |               | • IBM Prerequisite Scanner for Windows platform  
|     |               | Tivoli Asset Discovery for Distributed 7.2.2 reports package for Tivoli Common Reporting |

**Information regarding installing DB2**

Install DB2 before you start installing Tivoli Asset Discovery for Distributed. You can install it on the same or separate computer, depending on the size of your infrastructure.

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

- [Installing DB2 Version 9.1](#)
- [Installing DB2 Version 9.5](#)
- [Installing DB2 Version 9.7](#)

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

- [DB2 9.1](#)
- [DB2 9.5](#)
- [DB2 9.7](#)

To get the db2ese_o.lic license file uncompress the *IBM DB2 V9.7 Enterprise Server Edition Restricted Use Quick Start Guide and Activation for Linux, UNIX and Windows Multilingual* package (part number CZL3UML, file name DB2_ESE.Restricted_QS_Activation.97.zip) downloaded from Passport Advantage.
You can list all the DB2 products with available license information, including the product identifier by issuing the following command: `db2licm -l`.

Now, you can install Tivoli Asset Discovery for Distributed.

**Synchronizing the clocks of server and database computers**

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

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

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

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

**Procedure**

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

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

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

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

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

**Procedure**

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

**Installing in interactive mode**

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

1. “Preinstallation steps” on page 35
Before you start the installation, prepare installation images and install DB2. If you want to install the server and the database on different computers, synchronize the server and database clocks.

2. **Installing the server in interactive mode**
   Use the installation wizard to specify all parameters as the installation proceeds.

3. **Installing Tivoli Asset Discovery for Distributed in interactive mode on separate computers** on page 44
   If you have decided to install the database on a separate computer than the server, for example to improve the performance of the server, run the installer twice on each of the computers. Install DB2 before you run the installer on the designated computer.

4. **Verifying the interactive installation** on page 49
   Check the log files and start the Web user interface to verify that the server installation has been successful.

5. **Resuming a stopped or failed Asset Discovery for Distributed installation** on page 49
   There are three phases of server installation on embedded WebSphere Application Server: preinstallation, installation and postinstallation. If the installation fails or stops, there can be different ways to rerun it, depending on the phase or method used.

### Installing the server in interactive mode
Use the installation wizard to specify all parameters as the installation proceeds.

#### Before you begin
- You must have the following operating system privileges to install and run the server:
  - **UNIX**
    - root
  - **Windows**
    - Administrator
- On UNIX and Linux server computers, there must be graphical interface available, and the X server must be properly configured (the `DISPLAY` variable must be set properly). Otherwise, use **silent mode**.
- If you have downloaded the installation image from Passport Advantage, ensure that you have prepared your files for installation.
- Before you start the installation of the server you need to apply the DB2 license entitlement certificate. For information on how to do that refer to the topic **Registering a DB2 product or feature license key using the db2licm command** (DB2 9.1). To get the db2ese_0.11c license file uncompress the IBM DB2 Enterprise Server Edition 9.7 Restricted Use Activation package (part number CZL3UML), file name: DB2_ESE_Restricted_Activation_V97.zip (DVD), DB2_ESE_Restricted_QS_Activation_97.zip (Passport Advantage).

**Note:** Do not use underscore (‘_’) in the server installation host name. Even if you remove it from the host name after the installation of the server, you will have to reinstall DB2 to make the server work properly. For more information see **RFC 952**

#### Procedure
1. In the directory where you extracted the installation files, run **launchpad.exe** (Windows) or **launchpad.sh** (other platforms). The Welcome page opens. You can also launch the installation file
directly from the DIRECTORY_WITH_INSTALLATION_FILES\server. You do not need the web browser for this method. You are directed straight to the language selection window.

2. In the left navigation bar, click Install or upgrade to Tivoli Asset Discovery for Distributed.

3. Click Launch the server installation wizard. A splash screen opens.

4. Select the language of the installation and click OK. The installation wizard starts and the welcome panel opens. Click Next.

5. Accept the terms of the license agreement, and click Next. Specify the directory where you want to install Tivoli Asset Discovery for Distributed. Click Next.

6. On the new panel, specify the type of installation that you want:
   - For typical installation, select Production Environment.
   - For proof-of-concept installation, select Test Environment.

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

   **Note:** If you select Test environment, both components are installed on the local computer. Click Next.

7. Select the components that you want to install. You can install the server and database on the same computer or on different computers. If you have already installed a component on this computer, or you are running the proof-of-concept installation, that selection is unavailable and this panel does not appear.

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

8. If you have decided to install the server database, you must specify:
   - Windows The location of the DB2 instance.
   - UNIX Linux The home directory of the DB2 instance owner.

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

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

   Once the Checklist items are verified, you can proceed to the next panel by clicking Next.

9. If you have decided to install the server, you can accept or change the ports for communication with the server console and agents. The installer checks if the ports you selected are already in use. If there are any conflicts, or you duplicated the values for the ports, a message about the problem displays.
Click Next to start verification. Then click Next again to access the next panel.

10. If you have decided to install the server database, you must specify the password for the tlmsrv user, which is created during installation. 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, +, -, *, and |. The password is stored in an encrypted form in the application server configuration files. After you click Next, the password is validated for correctness. Additionally, the installation wizard searches for the existing server database in the selected DB2 instance. In case the server database is found, the installer verifies whether it can be used or migrated. If the database is not found, it is created.
If you have decided not to install the server database, you must specify the details of the connection to the remote server database. Select **Do not validate the remote database** if you plan to install it later.

11. Click **Next**. The installation wizard tries to open a JDBC connection using the provided values. Additionally, if the remote database was created by different version, or product, or it was created in a different mode, it is reported as a warning. Click **Next** to access the next panel.

12. Define the security settings:

**Use FIPS 140-2 cryptography**

This option is available only when you are installing the server. Select it to enable the encryption of data using approved algorithms from the Federal Information Processing Standard 140–2. This setting applies to the server that communicates with the agents.

**IBM i**

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

**Security Level**

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

**Attention:** For information about how to set the level of security before installing agents, refer to the topic [Performing agent security-related tasks](#).
13. Click **Next** and review the installation information. On the installation summary page, check the information that is provided and confirm that you have enough space to complete the installation. The creation of temporary files might require more space, than the total size shown. If the amount of available space is close to the total size shown, clear some space before proceeding. Click **Install** to install the product.

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

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

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

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

**Installing Tivoli Asset Discovery for Distributed in interactive mode on separate computers**

If you have decided to install the database on a separate computer than the server, for example to improve the performance of the server, run the installer twice on each of the computers. Install DB2 before you run the installer on the designated computer.

**Installing the database on a designated computer:**

**Before you begin**

Before you start the installation of the server you need to apply the DB2 license entitlement certificate. For information on how to do that refer to the topic
Registering a DB2 product or feature license key using the db2licm command (DB2 9.1). To get the db2ese_o.lic license file uncompress the IBM DB2 Enterprise Server Edition 9.7 Restricted Use Activation package (part number CZL3UML), file name:
DB2_ESE_Restricted_Activation_V97.zip (DVD),
DB2_ESE_Restricted_QS_Activation_97.zip (Passport Advantage).

If you start with the database installation, you will be able to test the connection between the server and the database. After the installation of both components is completed, the server will not need to be restarted to work. If you first install the server and then the database, you will need to restart the server.

Procedure
1. In the directory where you extracted the installation files, run launchpad.exe (Windows) or launchpad.sh (other platforms). The Welcome page opens. You can also launch the installation file
   - UNIX/TAD4D-server-7.2.2-your_platform.sh
   - Windows/TAD4D-server-7.2.2-your_platform.bat
   directly from the DIRECTORY_WITH_INSTALLATION_FILES\server. You do not need the Web browser for this method. You are directed straight to the language selection window.
2. In the left navigation bar, click Install or upgrade to Tivoli Asset Discovery for Distributed.
3. Click Launch the server installation wizard. A splash screen opens.
4. Select the language of the installation and click OK. The installation wizard starts and the welcome panel opens. Click Next.
5. Accept the terms of the license agreement, and click Next. Specify the directory where you want to install Tivoli Asset Discovery for Distributed. Click Next.
6. On the new panel, specify the type of installation that:
   - For a typical installation, select Production Environment.
   
   **Note:** Test mode enforces both components to be installed on local computer. Click Next.
7. Select the Database for administration server component and click Next.
8. On the next panel specify:
   - Windows DB2 installation directory
   - UNIX/LINUX The home directory of the DB2 instance owner.
   You can enter the location of DB2 manually or you can choose from the list of found DB2 instances. The dropdown list contains all local DB2 instances found, including those that are not supported. They are marked with a different color and you cannot select them.
   After you have clicked Next, the selected database will be verified and the verification results will be presented on the panel.
   Once the Checklist items are verified, you can proceed to the next panel by clicking Next.
9. Specify the password for the tlmsrv user, which is created during the installation. 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, +, -, *, and $. The password for the tlmsrv user is stored in an encrypted form in the application server configuration files. After you click Next, the
password is validated for correctness. Additionally, the installation wizard searches for the existing server database in the selected DB2 instance. In case the server database is found, the installer verifies whether it can be used. If the database is not found, it will be created.

10. Define the security settings:

**Security Level**

- If you set the minimum or medium security level, agents can communicate with the server by either the secure or the nonsecure port, depending on the security level that you define when you deploy agents.
- If you set the maximum security level, you must set the same level of security for all agents when you deploy them.
11. Click Next and review the installation information. On the installation summary page, check the information that is provided and confirm that there is enough space to complete the installation. The creation of temporary files might require more space than the total size shown. If the amount of available space is close to the total size shown, clear some space before proceeding. Click Install to install the database.

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

12. When the installation completes, click Done to exit the wizard.

**Installing the server on a separate computer:**

Install the server component on a computer different from the one on which DB2 is installed. Choose this interactive installation method to install the Tivoli Asset Discovery for Distributed server with embedded WebSphere Application Server.

**Before you begin**

On UNIX and Linux server computers, there must be graphical interface available, and the X server must be properly configured (the DISPLAY variable must be set properly). Otherwise, use silent mode.

**Note:** Do not use underscore ("_") in the server installation host name. Even if you remove it from the host name after the installation of the server, you will have to reinstall DB2 to make the server work properly. For more information see RFC 952.
Procedure

1. Repeat the steps 1 - 4 from the previous task. A new panel opens informing you that the database is already present on the computer. Click Next.

2. Specify the component to be installed. In this case, select the Administration server option. The database component, which is already installed, is grayed. Click Next.

3. Accept or change the ports for communication with the server console and agents. The installer checks if the ports you selected are already in use, and lets you know if there are any conflicts. Additionally, the installer will warn you if you have duplicated values for the ports.

   **Specify Communication Ports for Administration Server Web UI**
   - HTTP port 8899 (8899 is the default)
   - HTTPS port 8888 (8888 is the default)

   **Communication Ports with Agents**
   - Minimum security port 9988 (9988 is the default)
   - Medium security port 9999 (9999 is the default)
   - Maximum security port 9977 (9977 is the default)

   Click Reset to defaults

   On this panel you can provide all the ports that will be used to communicate with administration server console and agents

Click Next to start verification. Then, click Next to access the next panel.

4. Specify the connection details to the remote server database:

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

   **Port number**
   The port that is used by the instance of DB2 that is hosting the administration server database on the computer where this database is installed. The default is 50000.

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

   **Enter password**
   Provide the password for the tlmsrv user, which you created during the installation of the database.

Click Next. The installation wizard tries to open a JDBC connection using the provided values.
5. Click Next. The password is validated for correctness. Additionally, the installation wizard searches for the existing server database in the selected DB2 instance. In case the server database is found, the installer verifies whether it can be used or migrated.

6. Click Next to begin the installation of the server component. When the installation completes, click Done to exit the wizard.

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

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

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

**Procedure**

1. Open the msg_servers.log file and check if it contains the information that the application was successfully installed. By default, the file is stored under the following path: Tivoli_Common_Directory/COD/logs/install/message.

2. Access the login page at the following address: http://administration_server_IP_address:8899/ibm/console/login.do and check the Home page for information about any problems that might have occurred during installation.

   If the application is deployed on base WebSphere Application Server, the port number is specific for the profile.
   
   - **Windows** You can also open the login page from the system Start menu.

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

Perform the main configuration steps. See Configuring IBM Tivoli Asset Discovery for Distributed 7.2.2.

**Resuming a stopped or failed Asset Discovery for Distributed installation**
There are three phases of server installation on embedded WebSphere Application Server: preinstallation, installation and postinstallation. If the installation fails or stops, there can be different ways to rerun it, depending on the phase or method used.

**Procedure**

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

- If an error occurs during the **preinstallation** phase, you can restart the installation - no additional actions are necessary (valid for interactive and silent mode).
- If you encounter an error during the **installation** phase, you need to remove the installation directory and restart the installation.
- If an error occurs during the **postinstallation** phase, there are two ways to recover from it:
– If you can run the installer in interactive mode, follow the instructions in [Working with installation configuration steps](#).
– If you cannot run the installer in interactive mode, uninstall the product and install it again.

**Tip:** To find out the stage the installation stopped at, check the msg_server.log file and look for the following messages:
- CODIN0463I Preinstallation phase has begun.
- CODIN0464I Preinstallation phase has ended.
- CODIN0465I Installation phase has begun.
- CODIN0466I Installation phase has ended.
- CODIN0467I Postinstallation phase has begun.
- CODIN0468I Postinstallation phase has ended.

**Working with installation configuration steps:**

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

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

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

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

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

2. Review the most important information that is displayed in the top area of the dialog window. This dialog shows (among other things) the name, and location of the dedicated log file (if applicable).

3. Review the information shown in the lower part of the dialog window to determine the root cause of the problem.

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

```
Resolve tags (Succeeded)
Create user timsrv (Succeeded)
Set user password to never expire (Succeeded)
Populate the "TLMA" database (Failed)
Set properties: cli.properties (Succeeded)
Create profile (Succeeded)
Augment profile (Succeeded)
Deploy Admin application (Succeeded)
Deploy Message Handler application (Running)
Set up data sources (Ready)
```

**Command:** C:\Program Files\IBM\WebSphere\Administration\2.1\brooinstall.bat

**Purpose:** Create the "TLMA" database in selected DB2 instance and populate it with data

**Estimated duration:** 10 - 20 minutes

**Dedicated log file:** C:\WINDOWS\TEMP\trace_db_servers.log

To double-click on a log file, you can open the tab "Dedicated log" and then click on the log file you want to open.

---

**Running brooinstall.bat**

```
Current date: 2010-10-22
Current time: 10:00:01.70
```

---

**Completed 7 of 24 steps!**
4. Fix the problem.
5. On the installation panel, right-click the line that shows the problem, then click **Set > Ready (rerun the step)**.

The installer completes the step and the remaining dependent steps.

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

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

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

**Installing in silent mode**

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

1. **Preinstallation steps**
   Before you start the installation, prepare installation images and install DB2. If you want to install the server and the database on different computers, synchronize the server and database clocks.

2. “Installing the Tivoli Asset Discovery for Distributed server in silent mode” on page 53
   As an alternative to using the installation wizard, you can specify parameters in a response file and start the installation from the command line. Use this approach for unattended installation.

3. “Server installation response files” on page 54
   Response files provide input parameters that are used when you install from the command line or in silent mode.

4. “Verifying the silent installation” on page 57
Check the log files and start the Web user interface to verify that the server installation has been successful.

5. “Resuming a stopped or failed Asset Discovery for Distributed installation” on page 58

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

**Installing the Tivoli Asset Discovery for Distributed server in silent mode**

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

**Before you begin**

- You must have the following operating system privileges to install and run the server:
  - UNIX/Linux root
  - Windows Administrator
- Ensure that the `setupServers.bin` and `TAD4D-server-7.2.2-your_platform.sh` files have execution rights.
- If you have downloaded the installation image from Passport Advantage, ensure that you have prepared the files for installation.
- Before you start the installation of the server you need to apply the DB2 license entitlement certificate. For information on how to do that refer to the topic [Registering a DB2 product or feature license key using the db2licm command](DB2 9.1). To get the `db2ese_o.lic` license file uncompress the `DB2 Enterprise Server Edition V9.1 Restricted Use Activation` package (part number C150QML, file name `DB2_ESE_Restricted_Activation_V91.zip`) downloaded from Passport Advantage.

**Note:** Do not use underscore (‘_’) in the server installation host name. Even if you remove it from the host name after the installation of the server, you will have to reinstall DB2 to make the server work properly. For more information see [RFC 952](#).

To do this:

**Procedure**

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

**Important:** Ensure that the `RSP_LICENSE_ACCEPTED` parameter is uncommented and set to `true`. If you do not accept the license, the installation fails.

3. Navigate to the `DIRECTORY_WITH_INSTALLATION_FILES/server` directory. To start the installation, on the command line, run the following command:

   ```bash
   TAD4D-server-7.2.2-your_platform.sh -f response_file_path -i silent
   ```
where `response_file_path` is the absolute path to the response file you are using.

Example:
```
TAD4D-server-7.2.2-linux-ppc64.sh -f /tmp/image/
installResponseProduction.txt -i silent
```

- **Windows**
  ```
  TAD4D-server-7.2.2-your_platform.bat -f response_file_path
  -i silent
  ```
  where `response_file_path` is the absolute path to the response file you are using.
  
Example:
```
TAD4D-server-7.2.2-windows-x86_64.bat -f c:\image\installResponseProduction.txt -i silent
```

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

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

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

**Server installation response files**

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

There are two response files:
- `installResponseProduction.txt` used for installing in production mode
- `installResponsePOC.txt` used for installing in test (proof-of-concept) mode

Both are located in the directory `TAD4D-server-7.2.2-base/server/`. Some parameters have default values that you can accept or change. Others have no default, so you must provide a value.

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

**Common parameters**

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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter key name</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>License agreement acceptance</td>
<td>RSP_LICENSE_ACCEPTED</td>
<td>true</td>
</tr>
<tr>
<td></td>
<td>Delete the hash that flags this statement as a comment. The installation will fail if you do not explicitly agree with the license agreement by changing this statement from comment status.</td>
<td></td>
</tr>
</tbody>
</table>
Table 19. Response file parameters for all installations (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter key name</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Installation location</td>
<td>RSP_TLM_ROOT</td>
<td>- Windows: RSP_TLM_ROOT=C:\Program Files\IBM\LMT</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Linux/UNIX: RSP_TLM_ROOT=/opt/IBM/LMT</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Specify an empty directory where the selected elements will be installed. If the directory does not exist, it is created. If the directory path contains spaces, enclose it in double-quotiation marks.</td>
</tr>
<tr>
<td>Installation type</td>
<td>RSP_SETUP_TYPE</td>
<td>Admin</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Specify the type of installation to be performed. Possible values are:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Test: Installs the selected components in test (proof-of-concept) mode. Use this type of installation to quickly check if Tivoli Asset Discovery for Distributed is working and if it satisfies your business needs.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Admin: Installs the selected components in production mode.</td>
</tr>
<tr>
<td>Setup: administration</td>
<td>RSP_ADMIN_COMPONENT</td>
<td>true</td>
</tr>
<tr>
<td>server component selection</td>
<td></td>
<td>Specify whether or not the Tivoli Asset Discovery for Distributed server element should be installed. Possible values are:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- true: The server will be installed on this computer.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- false: The server will not be installed on this computer.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Note: This parameter is ignored during a proof-of-concept installation.</td>
</tr>
<tr>
<td>Setup: administration</td>
<td>RSP_ADMINDB_COMPONENT</td>
<td>true</td>
</tr>
<tr>
<td>database component selection</td>
<td></td>
<td>Specify whether or not the database element should be installed. Possible values are:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- true: The database will be installed on this computer.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- false: The database will not be installed on this computer.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Note: This parameter is ignored during a proof-of-concept installation.</td>
</tr>
<tr>
<td>Base configuration:</td>
<td>RSP_TLM_TLMSRV_PASSWD</td>
<td>Specify the password to be used to authenticate the access to the database by server processes. This password is assigned to a user with ID tlmsrv that is created on the target computer when a database element is installed for the first time. The password is also stored in an encrypted form in the properties file on the server computer.</td>
</tr>
<tr>
<td>tlmsrv user password</td>
<td></td>
<td>The maximum length is 20 characters and the characters allowed are: A-Z, a-z, 0-9, +, -, *, and</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Note: Passwords entered in this file are not encrypted. This may be a security violation in your organization.</td>
</tr>
</tbody>
</table>
### Table 19. Response file parameters for all installations (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter key name</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Base configuration:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ports used by administration server</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ports used by administration server</td>
<td></td>
<td></td>
</tr>
<tr>
<td>RSP_TLM_PORT</td>
<td></td>
<td>8899</td>
</tr>
<tr>
<td>The port used by the administration server console.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>RSP_TLM_SSL_PORT</td>
<td></td>
<td>8888</td>
</tr>
<tr>
<td>The port used by the administration server console in secure mode.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>RSP_TLM_MIN_SEC_PORT</td>
<td></td>
<td>9988</td>
</tr>
<tr>
<td>The port used for minimum security level communications.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>RSP_TLM_MED_SEC_PORT</td>
<td></td>
<td>9999</td>
</tr>
<tr>
<td>The port used for medium security level communications (HTTPS server authentication).</td>
<td></td>
<td></td>
</tr>
<tr>
<td>RSP_TLM_MAX_SEC_PORT</td>
<td></td>
<td>9977</td>
</tr>
<tr>
<td>The port used for maximum security level communications (HTTPS server and agent authentication).</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Note:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>If any of the selected ports is already used by a different application, the installation will fail. To continue the installation and resolve the problem later, uncomment the following parameter:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• RSP_DISABLE_COMMUNICATION_WARNINGS=true</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Server parameters

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

### Table 20. Parameters for silent installation of the Tivoli Asset Discovery for Distributed server

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter key name</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Administration server:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>remote administration database:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>address</td>
<td></td>
<td></td>
</tr>
<tr>
<td>RSP_TLM_DB_HOST</td>
<td></td>
<td>localhost</td>
</tr>
<tr>
<td>Supply the host name or the IP address where the administration server database will be installed. If you want to the database to be installed on the same computer as the server, set this parameter to localhost.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Note:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>This parameter is ignored during a proof-of-concept installation.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Administration database port number</td>
<td></td>
<td>30000</td>
</tr>
<tr>
<td>RSP_TLM_DB_PORT</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Specify the port number used to connect to the administration server database.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Note:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>This parameter is ignored during a proof-of-concept installation.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Database connection validation</td>
<td></td>
<td></td>
</tr>
<tr>
<td>RSP_DISABLE_DB_CONNECTION_TEST</td>
<td></td>
<td>false</td>
</tr>
<tr>
<td>Specify if the database connection is to be validated.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Note:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>This parameter is ignored during a proof-of-concept installation.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Setup: Use FIPS 140-2 cryptography</td>
<td></td>
<td></td>
</tr>
<tr>
<td>RSP_TLM_SERVER_FIPS_ENABLED</td>
<td></td>
<td>false</td>
</tr>
<tr>
<td>Specify whether FIPS-approved encryption algorithms are to be used. Possible values are:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>true</td>
<td>FIPS 140-2 approved cryptographic algorithms are used.</td>
<td></td>
</tr>
<tr>
<td>false</td>
<td>Default algorithms are used.</td>
<td></td>
</tr>
</tbody>
</table>
Database parameters

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

Table 21. Database parameters for silent installation

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter key name</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>IBM DB2 database server</strong></td>
<td>RSP_TLM_DB_PATH</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Specify where the DB2 database server is located. If you do not set this parameter, the installer will use the DB2 instance installed on the computer. If the installer detects more than one instance of DB2 on the computer, the installation will fail.</td>
<td></td>
</tr>
<tr>
<td><strong>Agent to server security level</strong></td>
<td>RSP_TLM_A2R_SEC_LEVEL</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>Determines the level of security to be used for communication between the agent and the server. This option is used only when installing the administration server database component. Possible values are:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>0</td>
<td>To use unsecure communication.</td>
</tr>
<tr>
<td></td>
<td>1</td>
<td>To use secure communications with server authentication.</td>
</tr>
<tr>
<td></td>
<td>2</td>
<td>To use secure communications with client and server authentication.</td>
</tr>
<tr>
<td><strong>Note:</strong></td>
<td>1. Agents with minimum (0) and medium (1) security levels can communicate with servers that have security levels of minimum or medium, provided that both the secure and unsecure ports are configured. If the maximum security level is used, both the agent and the server must be aligned with the security level set to maximum.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>2. If you select medium (1) or maximum (2) security, you must perform a series of tasks to set up and install certificates. For full information about enabling security, see the &quot;Security&quot; section of the Asset Discovery for Distributed infocenter.</td>
<td></td>
</tr>
</tbody>
</table>

Verifying the silent installation

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

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

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

**Procedure**

1. Open the msg_servers.log file and check if it contains the information that the application was successfully installed. By default, the file is stored under the following path: Tivoli_Common_Directory/COD/logs/install/message.

2. Access the login page at the following address: http://administration_server_IP_address:8899/ibm/console/login.do and check the Home page for information about any problems that might have occurred during installation.

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

- **Windows** You can also open the login page from the system Start menu.
3. Click **OK**. You do not need to provide any credentials at this stage.

Perform the main configuration steps. See *Configuring IBM Tivoli Asset Discovery for Distributed 7.2.2*.

**Resuming a stopped or failed Asset Discovery for Distributed installation**

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

**Procedure**

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

- If an error occurs during the **preinstallation** phase, you can restart the installation - no additional actions are necessary (valid for interactive and silent mode).
- If you encounter an error during the **installation** phase, you need to remove the installation directory and restart the installation.
- If an error occurs during the **postinstallation** phase, there are two ways to recover from it:
  - If you can run the installer in interactive mode, follow the instructions in *Working with installation configuration steps*.
  - If you cannot run the installer in interactive mode, uninstall the product and install it again.

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

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

**Working with installation configuration steps:**

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

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

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

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

**Procedure**

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

   ![Screenshot of installation progress window](screenshot.png)

   A dialog window opens.

2. Review the most important information that is displayed in the top area of the dialog window. This dialog provides, among other things, the name, and location of the dedicated log file (if applicable).

3. Review the information presented in the lower part of the dialog window to determine the root cause of the problem.

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

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

The installer completes the step and the remaining dependent steps.
If you have run the failed step outside the installation wizard, mark the step as completed successfully.

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

6. Click Next. The Postinstallation summary opens with information about installed components. Click Done to finish.
Installing Software Knowledge Base Toolkit

With a setup file that you copy to your computer, you can install both the content management server component and the raw data collector component.

It is recommended to install Software Knowledge Base Toolkit on a separate computer as catalog-related tasks are CPU resource-hungry. For information on how to do that refer to the installation instructions available in the product information center.

Taking the first steps after the installation of IBM Tivoli Software Knowledge Base Toolkit

Perform a few important tasks to configure Software Knowledge Base Toolkit to work with Tivoli Asset Discovery for Distributed.

Before you begin

You must have installed Tivoli Software Knowledge Base Toolkit in your infrastructure.

Perform the following steps to prepare the application to work with Tivoli Asset Discovery for Distributed:

Procedure

1. Download canonical XML catalog updates from the IBM website
2. Import the catalog
3. Publish the catalog so that it is available to Tivoli Asset Discovery for Distributed.

Installing IBM Tivoli Common Reporting

You can install Tivoli Common Reporting using any of three methods: wizard installation, console installation, or silent installation.

For information on how to install Tivoli Common Reporting refer to the installation instructions available in the product information center.

Moving the TLMA database to a separate server

You can move the IBM Tivoli Asset Discovery for Distributed database to a different computer to speed up the working of the server. This procedure applies only to the base WebSphere Application Server installations.

If your environment has grown after you first installed Tivoli Asset Discovery for Distributed, the larger number of agents reporting to the database can slow down the working of the server. To prevent this, move the database to a separate machine.

Ensure that the server and database computers are connected by a fast network connection, and that their clocks are synchronized.

You can move the TLMA database using the jacl script only to a computer which has the same operating system installed. For example, moving the database from a computer with Windows to a computer with Linux installed is not supported.

The wsadmin.bat (Windows) or wsadmin.sh (UNIX) command file is stored in the bin directory of your profile in WebSphere Application Server.
Procedure
1. Stop the Tivoli Asset Discovery for Distributed server.
2. On the Tivoli Asset Discovery for Distributed server create a backup of the TLMA database.
3. Run the Tivoli Asset Discovery for Distributed server installer and install the database component on the new computer. The installer creates an empty TLMA database which needs to be replaced.
4. On the new computer which is to perform the role of database server, restore the backup of the database that you have previously created.
5. On the Tivoli Asset Discovery for Distributed server, uninstall the database component and drop the database.
6. Copy the move_database.jacl script from the product DVD to a temporary directory on the Tivoli Asset Discovery for Distributed server or extract it from package downloaded from Passport Advantage. The file is stored in the scripts directory.
7. Edit the script file and provide the following parameters:
   - db_port
     The port number that will be used for server-database communication.
   - server_name
     The unique host name or IP address of the database server.
   - db_password
     The password for the tlmsrv user.
8. On the Tivoli Asset Discovery for Distributed server, start the wsadmin tool from a command prompt with the following command:
   - Linux
     ```shell
     was_home/profiles/profile_name/bin/wsadmin.bat
     ```
   - Windows
     ```shell
     was_home/profiles/profile_name/bin/wsadmin.sh
     ```
9. Change the configuration of the server data source to enable the server to connect to the database in its new location by running the following script: move_database.jacl path_to_dir_with_script

Troubleshooting server installation
Solve common problems that you might have encountered during server installation.

Troubleshooting server installation and uninstallation
This topic explains how to solve some common problems with the server installation, uninstallation, and upgrade.

Server installation problems on AIX operating system
Sometimes problems may occur during installation. Recognize the symptoms of the problem and find the solution.

The list below contains common installation problems that may occur on AIX platforms:

The server installed on an AIX platform does not start.
This problem is caused by a conflict of ports used by WebSphere Application Server. The problem and its workaround are documented in the Redbook: IBM WebSphere Application Server, version 5.0 System Management and Configuration, SG24-6195. Refer to sections 6.6.2 and
6.7.2, which deal with IP port conflicts. You can access the IBM Redbooks® publications from the following site: [http://www.redbooks.ibm.com](http://www.redbooks.ibm.com)

When installing on AIX, if you free disk space in one of the directories used during installation, the installation wizard does not refresh the space information.

  Restart the installation wizard.

While installing Asset Discovery for Distributed on AIX 6.1 with DB2 9.1, a DB2 installation error occurs.

  The `Tivoli_common_dir/COD/logs/install/trace/DB2install.log` file contains information on minor DB2 installation error: `ERROR:mkdev: 0514-519 The following device was not found in the customized device configuration database: name = 'aio0'

  ERROR: An error occurred while enabling Asynchronous I/O. DB2 requires Asynchronous I/O to be enabled to function properly. Enable this manually using "smit aio". If the problem persists contact a technical service representative. Select the step Installing DB2 as successful and continue the installation.

When you install the server manually on base WebSphere Application Server, the following error message appears in the log files: `ASYN0012E: Alarm/Timer threw exception`.

  The error is expected, and you should treat it as feedback about successful installation.

**Server installation problems on Solaris operating system**

Find the description that matches the problem you encounter and follow the instructions to solve it.

The list below contains descriptions of common problems that may occur when installing on the Solaris operating system:

**Installation of the server fails on a Sun workstation.**

  The following error is reported in the trace: Altering bufferpool SQL20189W The buffer pool operation (CREATE/ALTER) will not take effect until the next database startup due to insufficient memory (SQLSTATE=01657). Causes and solutions: The problem is related to the tuning of the shared memory available for the DB2 database. To solve the problem, increase the value of the shared memory (variable `shmsys:shminfo_shmmax`).

On the Solaris 10 SPARC server, installation fails during creating and populating the server. The `trace_db_servers.log` file contains the following message: SQL1478W The defined buffer pools could not be started. Instead, one small buffer pool for each page size supported by DB2 has been started. SQLSTATE=01626.

  The installation failed because kernel parameters on Solaris had not been set. The output from the `db2osconf` script in the DB2 installation directory shows the parameters with values that need to be set to allow the database to function properly. You can set these parameters in the `/etc/system` file. When you have set the parameters, restart the system and repeat the installation process.

When installing on Solaris or HP-UX operating systems, creating and populating the server database fails and the following error occurs: CODIN0035E An error occurred while populating the server database.

  The installation failed because of wrong `shmmx` parameter value. Use the `db2osconf` command to identify proper settings for this parameter. See the
Server installation fails on Solaris 10 SPARC platform during the creating and populating of the database. The following message is recorded in the trace_db_servers.log file: SQL3306N An SQL error "-1218" occurred while inserting a row into the table. SQL1218N There are no pages currently available in bufferpool "4096".

The problem may be caused by DB2 V9.1 or 9.5 self-tuning memory mechanism. It can be resolved by the installation of the latest DB2 fix pack. If the problem persists, disable Self-Tuning Memory Manager and configure DB2 manually. For more information refer to:


When you install the server manually on base WebSphere Application Server, the following error message appears in the log files: ASYN0012E: Alarm/Timer threw exception.

The error is expected, and you should treat it as feedback about successful installation.

Server installation problems on UNIX operating systems

Identify the problem with server installation that you are dealing with and the instructions how to solve it.

The list below contains descriptions of common installation problems on UNIX:

The installation wizard hangs when installing on Linux platforms.

A prerequisite for the Java Virtual Machine (JVM) is missing. Check the JVM prerequisites for the platform on which you are installing. See the Installation section for details.

Installation of a database on a UNIX platform fails when the installation path name includes double-byte characters. The script that creates the database fails to run when the installation path name includes double-byte characters. The database installation log, trace_db_servers.log, shows that the script failed because its path could not be interpreted. The path shown in the log file is garbled.

This problem occurs when the environment settings on the target computer are set incorrectly. Settings required to run scripts are obtained from the /etc/environment file. It is probable that this file includes the setting: LC_MESSAGES=C@lft. This setting restricts the characters that can be used in the environment to the ISO 8859-1 (ASCII) character set, and so double-byte characters cannot be used. To resolve this problem, comment out the LC_MESSAGES=C@lft setting and rerun the installation.

Installation of a database on a UNIX platform fails during the "Creating and populating the administration server database" phase. The trace_db_servers.log file shows that shared memory settings could not be allocated.

The shared memory settings are not sufficient. See the user documentation for your system for information about how to increase the shared memory size.

Following installation of a server on a UNIX platform, an attempt to log on to the server Web UI fails with a server initialization error.

This problem is caused by the failure of the installation wizard to create the tlmsrv user during the installation of the database. The reason for this failure is that the adduser command is not included in the $PATH variable.
To resolve the problem, use the adduser command to create the tlmsrv user on the computer where the database is installed. To avoid this problem happening again, ensure that the adduser command is included in the $PATH on all computers where you are planning to install a database.

**During the installation of a server on a UNIX platform, the tasks related to the creation of the databases fail and result in error.**

The step related to creating the databases results in error if the DB2 services are not running at the time of installation. The install wizard allows you to pause the installation, diagnose the problem, and run the failed step again. Refer to Tivoli Asset Discovery for Distributed: Planning, Installation, and Configuration, SC32-1431 for more information about resuming a failed installation. To solve the problem, start the DB2 services and resume the installation.

**Installation fails on UNIX because of the umask settings.**

Installation is not allowed to change system umask or force permissions to file systems such as /opt or /usr. Before you install, make sure that sufficient permissions are set on any subdirectories in file systems such as /opt or /usr. You must ensure that the DB2 administrator (typically db2inst1) has sufficient permissions to run scripts on this file systems (at least 755).

**On UNIX systems, when installing the server in interactive mode without graphical interface, the following message appears: The installer is unable to run in graphical mode. Try running the installer with the -console or -silent flag.**

- The -console option is not supported. If you run the installer with this option, an error will occur.
- To install the server in interactive mode on UNIX and Linux machines, there must be graphical interface available. Otherwise, you must use silent mode.

**Asset Discovery for Distributed Launchpad cannot be started on UNIX platforms.**

When starting the Asset Discovery for Distributed Launchpad from the hard disk of your UNIX computer, ensure that the path to the launchpad executable file (launchpad.sh) does not contain spaces.

**When you install the server manually on base WebSphere Application Server, the following error message appears in the log files: ASYN0012E: Alarm/Timer threw exception.**

- The error is expected, and you should treat it as feedback about successful installation.

**Server installation problems on Windows operating system**

Find the solution to the problem you encountered when installing on a Windows platform.

The list below contains descriptions of common problems that may occur on Windows operating system:

**The installation wizard running in unattended mode on a Windows platform does not recognize the presence of the DB2 server. If the installation wizard is used to install a database together.**

This problem occurs if the second installation is performed from the same command window as the first. At the end of the first installation, the command window environment is not updated with the information about the newly installed DB2 server. If a second installation is then performed
from the same window, it is unable to identify the presence of the DB2 server. If you run the second installation from a new command window, opened after the installation of the DB2 server has been completed, the problem is resolved.

The server installed on a Windows platform does not start.
This problem occurs when the server has been uninstalled prior to the installation, and the uninstallation has failed to complete the deregistration of the old server, so it is still pending. To resolve the problem of the pending deregistration, you must restart the computer. The new server can now be registered. You can do this as follows:
1. Open the file server_install_dir\admin\setup\setupAdmin.bat.
2. Copy the last line of the file and paste it into the command window.
3. Run the command.

When installing the server with DB2 on computers running Windows Server 2008, the installation of the database fails.
You must obtain DB2 DB2 9.1 Fix Pack 4 to install on Windows Server 2008 machines.

When you install the server manually on base WebSphere Application Server, the following error message appears in the log files: ASYN0012E: Alarm/Timer threw exception.
The error is expected, and you should treat it as feedback about successful installation.

The Launchpad does not start on a Windows computer
The following message is displayed:
The ordinal 325 could not be located in the dynamic link library SHDOCVW.dll.

The reason for this error might be that Internet Explorer is not fully initialized (registered). The problem appears only on computers with newly installed Windows operating system. To remedy the situation restart the server and then start the Launchpad again by running launchpad.exe.

Database problems
During server installation, problems with database may occur. Find the description of the problem and follow the instructions to solve it.

The list below contains descriptions of common database problems that may occur during installation:

When installing the server into an existing database server infrastructure, the installer does not recognize the password for the timsrv account (which is created automatically during installation).
This could happen for different reasons:
On Linux servers, if PAM (Pluggable Authentication Module) is not installed, you must install it.

For HP Unix trusted systems (according to Websphere Application Server - Express®, Version 6.0.x documentation) If you are using the local operating system user registry, HP-UX must be configured in untrusted mode. Trusted mode is not supported if global security is enabled using the local operating system user registry. See the following link for more information:
Server installation fails and the install log indicates that a DB2 command cannot be found. This could happen on AIX and Solaris computers, or UNIX systems in general.

Stop the installation and run the following: .~db2inst1/.profile. Restart the installation using -resume switch.

If the shell is set to /usr/bin/bash change the db2inst1 user's default shell to /usr/bin/ksh.

When installing the server with DB2 on computers running Windows Server 2008, the installation of the database fails.
You must obtain DB2 DB2 9.1 Fix Pack 4 to install on Windows Server 2008 machines.

The connection with the database cannot be established despite the fact that the values specified for the tlmsrv user, host name and port number are correct. The temp_dir/tad4d8.2.2.0/Server.log contains the following error message: A SQLException caught: java.net.ConnectException : Error opening socket to server <db2_host> on port <db2_port> with message : Connection timed out DB2ConnectionCorrelator: null.

Try to connect to the database using the DB2 client to find out more about the problem.

When installing the tlma database component the installer fails and the CODIN0154E message is displayed: The directory /tmp has not the required permissions set or the database instance owner is not valid.

If your DB2 instance owner home directory does not follow the pattern unix_home_dir/db2_instance_owner_name, create a symbolic link that will point to the DB2 instance owner home directory and select this symbolic link as an instance owner name during the installation. Example: If your DB2 instance owner is db2inst1 and its home directory is /home/db2, the installation will take db2 as the instance owner name. To fix it, create a symbolic link with /home/db2inst1 pointing to /home/db2 directory and then use /home/db2inst1 as the instance owner home directory in the installation wizard.

The installation, uninstallation, or upgrade of Asset Discovery for Distributed database fails and the cause of the failure is not known.

There might be different reasons for this, for example incorrect DB2 password or one that has just expired. Check the su.log file for possible reasons of the failure. Examples:

- Tue Dec 15 17:29:19 CET 2009 - Executing: su - db2inst4 -c "cd /opt/IBM/LMT/admin/db/db2 && ./dbinstall.sh true"
  su: Incorrect password
- Tue Dec 15 17:49:55 CET 2009 - Executing: su - db2inst4 -c "cd /opt/IBM/LMT/admin/db/db2 && .dbuninstall.sh"
  Password change requested. Choose a new password.
  Old Password:

For more information see Server installation and upgrade trace logs.

The installation of administration server fails during the "Populate the TLMA database" step and the following message is displayed: The database alias name already exists in either the local database directory or the system database directory.

This error happened after the DB2 instance containing database TLMA was uninstalled (the system database directory was not removed), and then
installed again, possibly in a new version. After installing the TLMA database, DB2 does not display the database, and an attempt to create it fails.

To remedy this error, perform the following steps:
1. Catalog the alias into the system database directory - run the command `db2 catalog database TLMA`.
2. If the newly installed instance is running on a higher version of DB2 (e.g. after the upgrade from version 9.1 to 9.7), the following command needs to be performed: `db2 migrate DATABASE tlma`.
3. Drop the database using the same alias - run the command `db2 drop database TLMA`.
4. Resume the failed installation, and rerun the "Populate the TLMA database" step.

**Execution of the migration script fails and the following message is displayed:**

CODINO329I Command completed with return code 4.

To solve the problem, set the DB2 parameter `DB2_EXTSECURITY` to `NO`, then create the DB2ADMNS and DB2USERS user groups, and restart the database. After you create those two groups, they will own permissions to files and folders, but the DB2 UDB will not perform an extra security checking.

For more information, see [DB2 UDB Security](#).

**Other installation problems**

If during the installation, you encountered a problem that is not platform-specific and does not suit any category of problems described in the “Server installation and uninstallation problems” section, look for the solution here.

The list below contains descriptions of common installation problems:

**Setup file cannot be launched while running the setupservers.bin file.**

You might not be logged on as the root. Log on again as the root and try again.

**Installation does not start and a message indicating that there is no supported JVM is displayed.** This problem occurs even when the supported JVM is present, when the system response is slow.

This problem is caused by a time out of the InstallAnywhere JVM verification routine. Relaunch the installation using the parameter `-is:jvmtimer <timeout in seconds>`. Specify a reasonably high number of seconds to avoid the time out. For example, start by trying 60 seconds and increase the time if the problem persists.

**The installation does not start - console mode detected.**

The situation occurs when the installation or uninstallation process stops right after its execution, and there is the Console mode detected entry in the ia.log or in the ServerUninstall.log file. You can also find in the trace_servers.log and in the msg_servers.log files the following error message: CODINO414E Console mode is not supported.

It means that you have tried to start the installation or uninstallation process interactively, however, you machine does not support any window system. Try to install such system, set the display appropriately or simply run the installation in the silent mode. For more information, see [Installing the server in silent mode](#) or [Uninstalling in silent mode](#).
The installation wizard will not run.

There are several reasons why this might happen:

- You do not have administrative privileges to the computer where you are trying to install the product. Ensure that you are logged on as an administrator (Windows) or root (UNIX).
- There is not enough disk space to create the necessary temporary files. Check the space available on the computer where you are installing the product.
- You are trying to install on a platform that is not supported.

The installation wizard will not finish.

If one of the last steps in the installation (for example, servers startup or chmod) fails, there might not be enough free memory.

Check the log file and look for OutOfMemoryError. In this case you can try freeing memory by: stopping Asset Discovery for Distributed servers; stopping the embedded WebSphere Application Server, and rerun the steps. You should consider that in this case you are at the memory limit and even if you are able to install the product, you can encounter problems when running it. Every Asset Discovery for Distributed server requires at least 770 MB free memory to deploy and 1 GB to run.

The installation has been broken and cannot be resumed.

Uninstall the server and install it again.

A Java core dump occurs during installation.

Out of memory errors can occur during the installation of the server causing a Java core dump.

If the out of memory condition prevents the installation from completing, increase the available memory to allow the installation to complete. The server requires at least 1GB free to deploy and 3GB to run with the database installed.

Installation fails because of a problem with temporary storage space.

The installation requires some free space in the /tmp directory and will fail if this space is not available. For more information, view the space requirements. If you cannot clear sufficient space in the /tmp directory, you can specify an alternative temporary file storage location when you launch the setup command. The syntax is: setupservers.bin -is:tempdir temp_dir.

No result record for a step in the Resume Installation panel.

If some invalid characters are present in the command STDOUT or STDERR, the installation will fail to create the result record associated with the failed step. In this situation the command standard output and command standard error is written to the log file and a dummy entry placed in the result record associated with the step. The information that is written to the log file can be used to diagnose the problem.

Installation fails because there is not enough disk space.

This is a known installation wizard problem, and also occurs during a silent installation. On AIX® systems the disk partitions are resized at runtime to accommodate the additional space requirements. The installation wizard caches the file system information when it starts, and it does not update this information while the install program is running. This can cause two effects:
The preview panel may claim that more space is needed than what is currently available (the preview panel however will also display the message: The following file systems will be expanded during the installation.

Because the disk space check is performed using cached information there is a possibility that disk space check operations will claim that there is enough space even when not enough space is available.

The server installation wizard displays the information that the master.tag file cannot be found and installation cannot continue even though the files have been removed from the file system.

The problem occurs because the appropriate entries have not been removed from the InstallAnywhere product registry. First, back the .com.zerog.registry.xml file up, and then manually remove all entries referring to Tivoli Asset Discovery for Distributed. The exact location of this directory depends on the operating system:

- /var/.com.zerog.registry.xml (UNIX-based systems)
- \Program Files\Zero G Registry\.com.zerog.registry.xml (Windows)

When the browser opens at the end of the installation of a server, the logon page of the Web UI is not found.

This can occur if the server has not correctly plugged in to WebSphere Application Server. To resolve the problem, you must regenerate the Web server plugin configurations. To do this, complete the following steps:

1. Start the WebSphere Administrator's Console.
2. In the navigation pane, click Environment Update Web Server Plugin.
3. On the page that is displayed, click OK.
4. Stop and restart the server.

Installation ends successfully but the server cannot be reached through the HTTP server.

On Windows, the WebSphere installation path and node name can be combined in a way that the Web server configuration fails because path names exceed the Windows limit. As a result, Asset Discovery for Distributed works only on WebSphere Application Server internal transports. Reinstall WebSphere Application Server shortening the path, then re-install Asset Discovery for Distributed.

Installation fails when started from a local machine.

If the installation of the server or the catalog manager is not initiated from the CD, but from a copy on the local machine, ensure that the path to the set up file does not contain special characters (for example, an exclamation mark), otherwise, the installation fails with an error. The following is an example of a path containing a special character: C:\|\Installation\TLM\setup\servers\setupServers.exe

Unable to uninstall the product whose installation process was broken during the installation phase.

When similar error message shows up during uninstallation to this one: java.lang.IllegalArgumentException: No product for ID=dc44d3c4-1ef2-11b2-afa7-66ef25df9157, you must delete the product file manually and start the installation process again.

While uninstalling the server, the Java process of the bundled WebSphere Application Server remains alive.

To uninstall the server, you must use the following files:
Problem with data sources initialization.
The following errors occur:

- An error message on Home page: An error that prevented the system from accessing the database occurred.
- If you use Test connection, you get an error message on License Metric Tool DataSource window: The test connection operation failed for data source LMT DataSource on server server1 at node NC143014Node02 with the following exception:
  java.sql.SQLException: [ibm][db2][jcc][t4][10205][11234] Null userid is not supported.DSRA0010E: SQL State = null, Error Code = -99,999. View JVM logs for further details.
- An error message with the ID CODDB3008E in the <Tivoli_common_dir>/logs/admin/message/msg.log file.

Restart the server.

The installation fails and the following message appears in the log file:
java.io.IOException: Not enough space at
java.lang.UNIXProcess.forkAndExec(Native Method).
The installation failed because of lack of memory. Increase the available memory to allow the installation to complete.

Remember: Close all running programs before you start the installation.

When performing the manual deployment of Asset Discovery for Distributed on base WebSphere Application Server a timeout appears.
The following two messages are displayed:
WASX7017E: Exception received while running file "installMessageHandler.jacl"; exception information: com.ibm.websphere.management.exception.ConfigServiceException
  com.ibm.websphere.management.exception.ConnectorException
  org.apache.soap.SOAPException: [SOAPException: faultCode=SOAP-ENV:Client; msg=Read timed out; targetException=java.net.SocketTimeoutException: Read timed out]
WASX7341W: No "save" was performed before the interactive scripting session exited; configuration changes will not be saved.
The script installMessageHandler has failed! Fix the problem and rerun the script by calling ./setupWAS.sh /opt/IBM/WebSphere/AppServer/ -s installMessageHandler

This usually happens on server computers that are heavily utilized. To properly deploy Asset Discovery for Distributed on base WebSphere Application Server without the timeout appearing perform the following steps:

1. Increase the value of com.ibm.SOAP.requestTimeout in soap.client.props. The file is stored in the following location:
   - /opt/IBM/WebSphere/AppServer/profiles/AppSrv01/properties/soap.client.props (Unix)
   - WAS_install_dir\IBM\WebSphere\AppServer\profiles\AppSrv01\properties\soap.client.props (Windows)

2. Execute the cleanup script:
   - cleanupWAS.sh (other platforms)
   - cleanupWAS.bat (Windows)

3. Execute the deployment script:
   - setupWAS.sh (other platforms)
• **setupWAS.bat** *(Windows)*

Detailed best practice information on how to configure the session timeout to a longer period of time and thus prevent disconnections can be found in the WebSphere Application Server information center at the following location: [http://publib.boulder.ibm.com/infocenter/wasinfo/v7r0/index.jsp?topic=/com.ibm.websphere.express.doc/info/exp/ae/rxml_atappmancommandsgroup.html](http://publib.boulder.ibm.com/infocenter/wasinfo/v7r0/index.jsp?topic=/com.ibm.websphere.express.doc/info/exp/ae/rxml_atappmancommandsgroup.html)

The **cleanupWAS** script fails while undeploying the administration server.

During the uninstallation, the **cleanupWAS** script fails while undeploying the Asset Discovery for Distributed administration server. In order to identify the problem, check the logs for the `FileNotFoundException` information. In order to successfully undeploy the server, restart WebSphere Application Server and run the script again.

The connection to the database fails during the installation process, even though user has provided the correct password for the `tlmsrv` login or the password is not accepted by the server installer.

The connection to the Asset Discovery for Distributed server database fails during the installation process, even though user has provided the correct password for the `tlmsrv` login (DB2 is to be reused). The user might also be asked to provide the password twice (which happens when the database is installed for the first time). The problem seems to be the binary for the pluggable authentication module, which probably is not working properly or it cannot start. To prevent the problem from occurring turn on the NO-PAM mode by setting the parameter `RSP_ENABLE_NO_PAM_MODE` to `true` in the server installation response file.

The installation of administration server fails because WebSphere Application Server does not allow creating profiles on servers which have a hostname with underscores or digits in the top level domain.

If you have installed WebSphere Application Server on a server with an underscore character or a digit in the server name, access the machine using its IP address. Next, install Asset Discovery for Distributed on a server with no underscore (`_`) in the hostname.

Examples:

• abc.def.com - accepted
• abc-def.com - accepted
• abc_def.com - not accepted
• abc.def.com1 - not accepted

After installing Software Knowledge Base Toolkit, no menu items are available in the portal.

When your Software Knowledge Base Toolkit installation finishes successfully and you try to log in to the web user interface for the first time, you might not see the Software Knowledge Base Toolkit available. To solve this problem, you must create a new user with appropriate rights:

1. Click **Users and Groups** > **Administrative User Roles**.
2. Click **Add** and select the roles for your user.
3. Log out and log in with the new user.
Chapter 3. Installing agents

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

Are you going to use your own tools to install agents?

- NO
- YES

1. **Plan the installation of your agents**. Most importantly, check the hardware and software prerequisites (REQUIRED)

2. **Perform agent preinstallation tasks** (OPTIONAL)

3. **Performing agent security-related tasks** (OPTIONAL)
   Depending on your software and the security level you selected while installing the administration server, there are several tasks you need to perform before you install the agents.

4. Install agents on computers that you want to monitor (REQUIRED)
   IBM Tivoli Asset Discovery for Distributed provides several methods for installing the agents on the computers that you want to monitor.

**AGENT INSTALLATION METHODS:**

- You might want to use your own tools to install agents in bulk. This method is intended for advanced administrators who want to write their own scripts or use existing commercial tools for installing a great number of agents. It utilizes native installation tools.
- Install using **Tivoli Configuration Manager**. This method is available on all supported platforms and is suitable for environments where Configuration Manager is installed.
- Install using **native installers**. This method is available on all supported platforms:
  - AIX
  - HP-UX
  - IBM i
  - Linux
  - Linux on System z
  - Solaris
  - Windows

   It also allows to install agents silently.
   **You might also want to install agents using** **Windows Logon Scripts**. This method is suitable for topologies where a lot of Windows agents are to be installed.

- Install using **shell installers** (UNIX platforms only). It is not necessary to edit and copy the response file to the target directory. All the parameters that you supply are validated on the run.

If any problems occurred, **start troubleshooting the agent installation(s)**.
Planning the installation of agents

The topics in this section contain information about hardware and software prerequisites that need to be fulfilled when installing Tivoli Asset Discovery for Distributed agents. The requirements were determined in previous releases of Tivoli Asset Discovery for Distributed.

Supported operating systems for agents

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

Supported versions of IBM AIX

<table>
<thead>
<tr>
<th>Version</th>
<th>Required level, service packs, patches</th>
<th>Supported partitioning technologies</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.1</td>
<td>LPAR</td>
<td>LPAR, PowerVM® - DLPAR, PowerVM - Single Shared Processor Pool, PowerVM - Micro-Partitioning®, PowerVM - Multiple Shared Processor Pools, PowerVM - Shared Dedicated Processor, System WPARs (both regulated and un-regulated, also RSET bound), Application WPARs, LPAR mobility (Live Partition Mobility), IBM zEnterprise® BladeCenter Extension (zBX), Processor Core Deconfiguration</td>
</tr>
<tr>
<td>6.1</td>
<td>APAR IZ49636 - this fix is required if you are installing the agent in a WPAR environment. If you are installing the agent in a WPAR environment and using WPAR or LPAR mobility or relocation, the AIX 6.1 instance needs to be upgraded to Technology Level 3 or later. AIX Technology Level 6100-02-03-0909 or higher is recommended in both LPARs between which a WPAR (with an agent installed) is being relocated.</td>
<td>LPAR, PowerVM - DLPAR, PowerVM - Single Shared Processor Pool, PowerVM - Micro-Partitioning, PowerVM - Multiple Shared Processor Pools, PowerVM - Shared Dedicated Processor, System WPARs (both regulated and un-regulated, also RSET bound), Application WPARs, LPAR mobility (Live Partition Mobility), WPAR mobility (Live Application Mobility), IBM zEnterprise BladeCenter Extension (zBX), Processor Core Deconfiguration</td>
</tr>
<tr>
<td>5.3</td>
<td>xIC.aix50.rte.6.0.0.3 or later Maintenance Level 3 to support sub capacity pricing on Power® 5 Note: Maintenance Level 3 is a minimum requirement, but use Technology Level 7 to support Multiple Processor Shared Pools. Technology Level 7 or later for LPAR mobility</td>
<td>LPAR, PowerVM - DLPAR, PowerVM - Single Shared Processor Pool, PowerVM - Micro-Partitioning, PowerVM - Multiple Shared Processor Pools, PowerVM - Shared Dedicated Processor, LPAR mobility (Live Partition Mobility), IBM zEnterprise BladeCenter Extension (zBX), Processor Core Deconfiguration</td>
</tr>
<tr>
<td>5.2</td>
<td>xIC.aix50.rte.6.0.0.3 or later APAR IY51805 procfiles</td>
<td>LPAR, PowerVM - Single Shared Processor Pool, IBM zEnterprise BladeCenter Extension (zBX)</td>
</tr>
</tbody>
</table>
Tivoli Asset Discovery for Distributed agents can also be deployed on Virtual I/O Server (VIOS) version 2.2 and higher. The deployment procedure is the same as the standard one. For more information, see “Installing agents on AIX using native installers” on page 104.

**Supported versions of HP-UX**

<table>
<thead>
<tr>
<th>Version</th>
<th>Required level, service packs, patches</th>
<th>Supported partitioning technologies</th>
</tr>
</thead>
<tbody>
<tr>
<td>11i v3 on PA-RISC</td>
<td>Quality Pack Depot for 11i v2, September 2006, PHKL_35709 (s700_800 11.23 pthread_con_wait, hires timers, callout), PHCO_39699 (s700_800 11.23 pthread library cumulative patch)</td>
<td>nPAR, vPAR</td>
</tr>
<tr>
<td>11i v2 on PA-RISC 64-bit (in 32-bit compatibility mode)</td>
<td>Quality Pack Depot for 11i v2, September 2006, PHKL_35709 (s700_800 11.23 pthread_con_wait, hires timers, callout), PHCO_39699 (s700_800 11.23 pthread library cumulative patch)</td>
<td>HP Integrity Virtual Machines 4.0, 4.1, 4.2, nPAR, vPAR, iCAPv9</td>
</tr>
<tr>
<td>11i v3 on Itanium 2 Integrity Server</td>
<td>Quality Pack Depot for 11i v2, September 2006, PHKL_35709 (s700_800 11.23 pthread_con_wait, hires timers, callout), PHCO_39699 (s700_800 11.23 pthread library cumulative patch)</td>
<td>HP Integrity Virtual Machines 4.0, 4.1, 4.2</td>
</tr>
<tr>
<td>11i v2 on Itanium 2 Integrity Server</td>
<td>Quality Pack Depot for 11i v2, September 2006, PHKL_35709 (s700_800 11.23 pthread_con_wait, hires timers, callout), PHCO_39699 (s700_800 11.23 pthread library cumulative patch)</td>
<td>nPAR, vPAR, iCAPv9</td>
</tr>
<tr>
<td>11i v1 for PA-RISC</td>
<td>PHSS_26946, PHSS_33033, PHCO_34275</td>
<td>nPAR, vPAR</td>
</tr>
</tbody>
</table>

**Supported versions of IBM i**

<table>
<thead>
<tr>
<th>Version</th>
<th>Required level, service packs, patches</th>
<th>Supported partitioning technologies</th>
</tr>
</thead>
<tbody>
<tr>
<td>V7R1</td>
<td>PTF SE8154 for 5770SS1, Options 13 and 30 of 5770SS1</td>
<td>LPAR, PowerVM - DLPAR, PowerVM - Single Shared Processor Pool, PowerVM - Micro-Partitioning, PowerVM - Multiple Shared Processor Pools, PowerVM - Shared Dedicated Processor</td>
</tr>
<tr>
<td>V6R1</td>
<td>PTF SE8115 for 5761SS1, Options 13 and 30 of 5761SS1, LIC PTF MF46769 (if you are using secure communication)</td>
<td>LPAR, PowerVM - DLPAR, PowerVM - Single Shared Processor Pool, PowerVM - Micro-Partitioning, PowerVM - Multiple Shared Processor Pools, PowerVM - Shared Dedicated Processor</td>
</tr>
<tr>
<td>V5R4</td>
<td>PTF SE8116 for 5722SS1, Options 13 and 30 of 5722SS1, Crypto Access Provider 128-bit, PID: 5722AC3 (if secure communication is to be used)</td>
<td>LPAR, PowerVM - DLPAR, PowerVM - Single Shared Processor Pool, PowerVM - Micro-Partitioning, PowerVM - Multiple Shared Processor Pools, PowerVM - Shared Dedicated Processor</td>
</tr>
</tbody>
</table>

**Supported versions of Red Hat Enterprise Linux**
<table>
<thead>
<tr>
<th>Version</th>
<th>Required level, service packs, patches</th>
<th>Supported partitioning technologies</th>
</tr>
</thead>
</table>
| 6 for Intel/AMD x86 (64-bit)  | compat-libstdc++-33 (32 and 64-bit)                                           | VMware ESX 4 - Single Server, Cluster, Mobility (VMware Vmotion)  
VMware ESXi 4 - Single Server, Cluster, Mobility (VMware Vmotion)  
VMware ESX 4.1 - Single Server, Cluster, Mobility (VMware Vmotion)  
VMware ESXi 4.1 - Single Server, Cluster, Mobility (VMware Vmotion)  
VMware vSphere 5 - Single Server, Cluster, Mobility (VMware Vmotion)  
Fix Pack 2 VMware vSphere 5.1 - Single Server, Cluster, Mobility (VMware Vmotion)  
Fix Pack 2 VMware vSphere 5.5 - Single Server, Cluster, Mobility (VMware Vmotion)  
BIOS (SMBIOS 2.5 or higher) & Operating System boot core limit  
System scaling using Intel QuickPath Interconnect                                                                 |
| 6 for Intel/AMD x86 (32-bit)  | compat-libstdc++-33 (32-bit)                                                 | VMware ESX 4 - Single Server, Cluster, Mobility (VMware Vmotion)  
VMware ESXi 4 - Single Server, Cluster, Mobility (VMware Vmotion)  
VMware ESX 4.1 - Single Server, Cluster, Mobility (VMware Vmotion)  
VMware ESXi 4.1 - Single Server, Cluster, Mobility (VMware Vmotion)  
VMware vSphere 5 - Single Server, Cluster, Mobility (VMware Vmotion)  
Fix Pack 2 VMware vSphere 5.1 - Single Server, Cluster, Mobility (VMware Vmotion)  
Fix Pack 2 VMware vSphere 5.5 - Single Server, Cluster, Mobility (VMware Vmotion)  
BIOS (SMBIOS 2.5 or higher) & Operating System boot core limit  
System scaling using Intel QuickPath Interconnect                                                                 |
| 6 for IBM Power Systems (64-bit) | compat-libstdc++-33 (32 and 64-bit) Update 1 or later for LPAR mobility       | LPAR  
PowerVM - DLPAR  
PowerVM - Single Shared Processor Pool  
PowerVM - Micro-Partitioning  
LPAR mobility (Live Partition Mobility)  
Processor Factory Deconfiguration                                                                                                          |
| 6 for IBM System z (31-bit) on 64-bit hardware | compat-libstdc++-33                                                         | LPAR  
z/VM®  
Parallel Sysplex®  
Unified Resource Manager (URM)  
IBM Multi-System Manager (MOM)  
IBM Single System Manager (SSM)  
IBM Workload Enhancer (WLE)  
Processor Factory Deconfiguration                                                                                                          |
| 5 for Intel/AMD x86 (64-bit)  | compat-libstdc++-33 (32 and 64-bit)                                           | VMware ESX 3.0 - Single Server, Cluster, Mobility (VMware Vmotion)  
VMware ESXi 3.5 - Single Server, Cluster, Mobility (VMware Vmotion)  
VMware ESX 4 - Single Server, Cluster, Mobility (VMware Vmotion)  
VMware ESXi 4 - Single Server, Cluster, Mobility (VMware Vmotion)  
VMware ESX 4.1 - Single Server, Cluster, Mobility (VMware Vmotion)  
VMware ESXi 4.1 - Single Server, Cluster, Mobility (VMware Vmotion)  
VMware vSphere 5 - Single Server, Cluster, Mobility (VMware Vmotion)  
Fix Pack 2 VMware vSphere 5.1 - Single Server, Cluster, Mobility (VMware Vmotion)  
Fix Pack 2 VMware vSphere 5.5 - Single Server, Cluster, Mobility (VMware Vmotion)  
BIOS (SMBIOS 2.5 or higher) & Operating System boot core limit  
System scaling using Intel QuickPath Interconnect  
Microsoft Hyper-V Server 2008 R2  
Microsoft Hyper-V Server 2012                                                                                                           |
<table>
<thead>
<tr>
<th>Version</th>
<th>Required level, service packs, patches</th>
<th>Supported partitioning technologies</th>
</tr>
</thead>
<tbody>
<tr>
<td>5 for Intel/AMD x86 (32-bit)</td>
<td>compat-libstdc++-33 (32-bit)</td>
<td>VMware ESX 2.5 - Single Server, Server Farm, Mobility (VMware Vmotion)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>VMware ESX 3.0 - Single Server, Cluster, Mobility (VMware Vmotion)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>VMware ESX 3.5 - Single Server, Cluster, Mobility (VMware Vmotion)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>VMware ESXi 3.5 - Single Server, Cluster, Mobility (VMware Vmotion)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>VMware ESX 4 - Single Server, Cluster, Mobility (VMware Vmotion)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>VMware ESXi 4 - Single Server, Cluster, Mobility (VMware Vmotion)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>VMware ESX 4.1 - Single Server, Cluster, Mobility (VMware Vmotion)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>VMware ESXi 4.1 - Single Server, Cluster, Mobility (VMware Vmotion)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>VMware vSphere 5 - Single Server, Cluster, Mobility (VMware Vmotion)</td>
</tr>
<tr>
<td></td>
<td>Fix Pack 2</td>
<td>VMware vSphere 5.1 - Single Server, Cluster, Mobility (VMware Vmotion)</td>
</tr>
<tr>
<td></td>
<td>Fix Pack 2</td>
<td>VMware vSphere 5.5 - Single Server, Cluster, Mobility (VMware Vmotion)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>BIOS (SMBIOS 2.5 or higher) &amp; Operating System boot core limit</td>
</tr>
<tr>
<td></td>
<td></td>
<td>System scaling using Intel QuickPath Interconnect</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Microsoft Hyper-V Server 2008 R2</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Microsoft Hyper-V Server 2012</td>
</tr>
<tr>
<td>5 for IBM Power Systems (64-bit)</td>
<td>compat-libstdc++-33 (32 and 64-bit)</td>
<td>LPAR</td>
</tr>
<tr>
<td></td>
<td>Update 1 or later for LPAR mobility</td>
<td>PowerVM - DLPAR</td>
</tr>
<tr>
<td></td>
<td></td>
<td>PowerVM - Single Shared Processor Pool</td>
</tr>
<tr>
<td></td>
<td></td>
<td>PowerVM - Micro-Partitioning</td>
</tr>
<tr>
<td></td>
<td></td>
<td>LPAR mobility (Live Partition Mobility)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Processor Factory Deconfiguration</td>
</tr>
<tr>
<td>5 for IBM System z (31-bit) on 64-bit hardware</td>
<td>compat-libstdc++-33</td>
<td>LPAR</td>
</tr>
<tr>
<td></td>
<td></td>
<td>z/VM</td>
</tr>
<tr>
<td>ES/AS/WS 4 for Intel/AMD x86 (64-bit)</td>
<td>compat-libstdc++-33 (32 and 64-bit)</td>
<td>VMware ESX 2.5 - Single Server, Server Farm, Mobility (VMware Vmotion)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>VMware ESX 3.0 - Single Server, Cluster, Mobility (VMware Vmotion)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>VMware ESX 3.5 - Single Server, Cluster, Mobility (VMware Vmotion)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>VMware ESXi 3.5 - Single Server, Cluster, Mobility (VMware Vmotion)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>VMware ESX 4 - Single Server, Cluster, Mobility (VMware Vmotion)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>VMware ESXi 4 - Single Server, Cluster, Mobility (VMware Vmotion)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>VMware ESX 4.1 - Single Server, Cluster, Mobility (VMware Vmotion)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>VMware ESXi 4.1 - Single Server, Cluster, Mobility (VMware Vmotion)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>VMware vSphere 5 - Single Server, Cluster, Mobility (VMware Vmotion)</td>
</tr>
<tr>
<td></td>
<td>Fix Pack 2</td>
<td>VMware vSphere 5.1 - Single Server, Cluster, Mobility (VMware Vmotion)</td>
</tr>
<tr>
<td></td>
<td>Fix Pack 2</td>
<td>VMware vSphere 5.5 - Single Server, Cluster, Mobility (VMware Vmotion)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>BIOS (SMBIOS 2.5 or higher) &amp; Operating System boot core limit</td>
</tr>
<tr>
<td></td>
<td></td>
<td>System scaling using Intel QuickPath Interconnect</td>
</tr>
<tr>
<td>ES/AS/WS 4 for Intel/AMD x86 (32-bit)</td>
<td>Compatibility packs: 1. libgcc-3.4.3-9 (32-bit) 2. compat-libstdc++-33 (32-bit, must be installed in the specified order)</td>
<td>VMware ESX 2.5 - Single Server, Server Farm, Mobility (VMware Vmotion)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>VMware ESX 3.0 - Single Server, Cluster, Mobility (VMware Vmotion)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>VMware ESX 3.5 - Single Server, Cluster, Mobility (VMware Vmotion)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>VMware ESXi 3.5 - Single Server, Cluster, Mobility (VMware Vmotion)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>VMware ESX 4 - Single Server, Cluster, Mobility (VMware Vmotion)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>VMware ESXi 4 - Single Server, Cluster, Mobility (VMware Vmotion)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>VMware ESX 4.1 - Single Server, Cluster, Mobility (VMware Vmotion)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>VMware ESXi 4.1 - Single Server, Cluster, Mobility (VMware Vmotion)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>VMware vSphere 5 - Single Server, Cluster, Mobility (VMware Vmotion)</td>
</tr>
<tr>
<td></td>
<td>Fix Pack 2</td>
<td>VMware vSphere 5.1 - Single Server, Cluster, Mobility (VMware Vmotion)</td>
</tr>
<tr>
<td></td>
<td>Fix Pack 2</td>
<td>VMware vSphere 5.5 - Single Server, Cluster, Mobility (VMware Vmotion)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>BIOS (SMBIOS 2.5 or higher) &amp; Operating System boot core limit</td>
</tr>
<tr>
<td></td>
<td></td>
<td>System scaling using Intel QuickPath Interconnect</td>
</tr>
<tr>
<td>Version</td>
<td>Required level, service packs, patches</td>
<td>Supported partitioning technologies</td>
</tr>
<tr>
<td>---------</td>
<td>----------------------------------------</td>
<td>-------------------------------------</td>
</tr>
</tbody>
</table>
| AS, version 4 for IBM Power Systems (64-bit) | Compatibility packs: 1. libgcc-3.4.3-9 (32-bit) 2. compat-libstdc++-33 (32 or 64-bit, must be installed in the specified order) | LPAR  
PowerVM - DLPAR  
PowerVM - Single Shared Processor Pool  
PowerVM - Micro-Partitioning |
| AS, version 4 for IBM System z (64-bit) | | LPAR  
z/VM |
| AS, version 4 for IBM System z (31-bit ) on 64-bit hardware | compat-libstdc++-33 | LPAR  
z/VM |

**Supported versions of Red Hat Linux Desktop**

<table>
<thead>
<tr>
<th>Version</th>
<th>Required level, service packs, patches</th>
<th>Supported partitioning technologies</th>
</tr>
</thead>
</table>
| 6 for Intel/AMD x86 (64-bit) | compat-libstdc++-33 (32 and 64-bit) | VMware ESX 4 - Single Server, Cluster, Mobility (VMware Vmotion)  
VMware ESX 4 - Single Server, Cluster, Mobility (VMware Vmotion)  
VMware ESX 4.1 - Single Server, Cluster, Mobility (VMware Vmotion)  
VMware ESX 4.1 - Single Server, Cluster, Mobility (VMware Vmotion)  
VMware vSphere 5 - Single Server, Cluster, Mobility (VMware Vmotion)  
**Fix Pack 2** VMware vSphere 5.1 - Single Server, Cluster, Mobility (VMware Vmotion)  
**Fix Pack 2** VMware vSphere 5.5 - Single Server, Cluster, Mobility (VMware Vmotion)  
BIOS (SMBIOS 2.5 or higher) & Operating System boot core limit  
System scaling using Intel QuickPath Interconnect |
| 6 for Intel/AMD x86 (32-bit) | compat-libstdc++-33 (32-bit) | VMware ESX 4 - Single Server, Cluster, Mobility (VMware Vmotion)  
VMware ESX 4 - Single Server, Cluster, Mobility (VMware Vmotion)  
VMware ESX 4.1 - Single Server, Cluster, Mobility (VMware Vmotion)  
VMware ESX 4.1 - Single Server, Cluster, Mobility (VMware Vmotion)  
VMware vSphere 5 - Single Server, Cluster, Mobility (VMware Vmotion)  
**Fix Pack 2** VMware vSphere 5.1 - Single Server, Cluster, Mobility (VMware Vmotion)  
**Fix Pack 2** VMware vSphere 5.5 - Single Server, Cluster, Mobility (VMware Vmotion)  
BIOS (SMBIOS 2.5 or higher) & Operating System boot core limit  
System scaling using Intel QuickPath Interconnect |
| version 5 for Intel/AMD x86 (32-bit) | compat-libstdc++-33 (32-bit) | VMware ESX 3.0 - Single Server, Cluster, Mobility (VMware Vmotion)  
VMware ESX 3.5 - Single Server, Cluster, Mobility (VMware Vmotion)  
VMware ESXi 3.5 - Single Server, Cluster, Mobility (VMware Vmotion) |
| version 4 for Intel/AMD x86 (32-bit) | compat-libstdc++-33 (32-bit) | VMware ESX 2.5 - Single Server, Server Farm, Mobility (VMware Vmotion)  
VMware ESX 3.0 - Single Server, Cluster, Mobility (VMware Vmotion)  
VMware ESX 3.5 - Single Server, Cluster, Mobility (VMware Vmotion)  
VMware ESXi 3.5 - Single Server, Cluster, Mobility (VMware Vmotion) |
<table>
<thead>
<tr>
<th>Version</th>
<th>Required level, service packs, patches</th>
<th>Supported partitioning technologies</th>
</tr>
</thead>
<tbody>
<tr>
<td>11 for Intel/AMD x86 (64-bit)</td>
<td>libstdc++-33-32bit-3.3.3-11.9.x86_64.rpm</td>
<td>VMware ESX 4 - Single Server, Cluster, Mobility (VMware Vmotion) VMware ESXi 4 - Single Server, Cluster, Mobility (VMware Vmotion) VMware ESX 4.1 - Single Server, Cluster, Mobility (VMware Vmotion) VMware ESXi 4.1 - Single Server, Cluster, Mobility (VMware Vmotion) VMware vSphere 5 - Single Server, Cluster, Mobility (VMware Vmotion) <strong>Fix Pack 2</strong> VMware vSphere 5.1 - Single Server, Cluster, Mobility (VMware Vmotion) <strong>Fix Pack 2</strong> VMware vSphere 5.5 - Single Server, Cluster, Mobility (VMware Vmotion) BIOS (SMBIOS 2.5 or higher) &amp; Operating System boot core limit System scaling using Intel QuickPath Interconnect Microsoft Hyper-V R2 Microsoft Hyper-V Server 2012</td>
</tr>
<tr>
<td>11 for Intel/AMD x86 (32-bit)</td>
<td>Service Pack 2 for Microsoft Hyper-V Server 2012</td>
<td>VMware ESX 4 - Single Server, Cluster, Mobility (VMware Vmotion) VMware ESXi 4 - Single Server, Cluster, Mobility (VMware Vmotion) VMware ESX 4.1 - Single Server, Cluster, Mobility (VMware Vmotion) VMware ESXi 4.1 - Single Server, Cluster, Mobility (VMware Vmotion) VMware vSphere 5 - Single Server, Cluster, Mobility (VMware Vmotion) <strong>Fix Pack 2</strong> VMware vSphere 5.1 - Single Server, Cluster, Mobility (VMware Vmotion) <strong>Fix Pack 2</strong> VMware vSphere 5.5 - Single Server, Cluster, Mobility (VMware Vmotion) BIOS (SMBIOS 2.5 or higher) &amp; Operating System boot core limit System scaling using Intel QuickPath Interconnect Microsoft Hyper-V R2 Microsoft Hyper-V Server 2012</td>
</tr>
<tr>
<td>11 for IBM Power Systems (64-bit)</td>
<td>LPAR PowerVM - DLPAR PowerVM - Single Shared Processor Pool PowerVM - Micro-Partitioning LPAR mobility (Live Partition Mobility) Processor Factory Deconfiguration</td>
<td></td>
</tr>
<tr>
<td>11 for IBM System z (64-bit) on 64-bit hardware</td>
<td>LPAR z/VM</td>
<td></td>
</tr>
<tr>
<td>10 for Intel/AMD x86 (32-bit and 64-bit)</td>
<td>compat-libstdc++ (32 and 64-bit)</td>
<td>VMware ESX 3.0 - Single Server, Cluster, Mobility (VMware Vmotion) VMware ESX 3.5 - Single Server, Cluster, Mobility (VMware Vmotion) VMware ESXi 3.5 - Single Server, Cluster, Mobility (VMware Vmotion) VMware ESX 4 - Single Server, Cluster, Mobility (VMware Vmotion) VMware ESXi 4 - Single Server, Cluster, Mobility (VMware Vmotion) VMware ESX 4.1 - Single Server, Cluster, Mobility (VMware Vmotion) VMware ESXi 4.1 - Single Server, Cluster, Mobility (VMware Vmotion) VMware vSphere 5 - Single Server, Cluster, Mobility (VMware Vmotion) <strong>Fix Pack 2</strong> VMware vSphere 5.1 - Single Server, Cluster, Mobility (VMware Vmotion) <strong>Fix Pack 2</strong> VMware vSphere 5.5 - Single Server, Cluster, Mobility (VMware Vmotion) BIOS (SMBIOS 2.5 or higher) &amp; Operating System boot core limit System scaling using Intel QuickPath Interconnect Microsoft Hyper-V 2008 Microsoft Hyper-V Server 2008 R2 Microsoft Windows Server 2008 R2 with Hyper-V Role Microsoft Windows Server 2008 R2 Hyper-V</td>
</tr>
</tbody>
</table>
## Supported versions of SUSE Linux Enterprise Desktop

<table>
<thead>
<tr>
<th>Version</th>
<th>Required level, service packs, patches</th>
<th>Supported partitioning technologies</th>
</tr>
</thead>
<tbody>
<tr>
<td>11 for Intel/AMD x86 (32-bit)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>11 for Intel/AMD x86 (64-bit)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>10 for Intel/AMD x86 (32-bit)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>10 for Intel/AMD x86 (64-bit)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Supported versions of SUSE Linux Enterprise Desktop**

<table>
<thead>
<tr>
<th>Version</th>
<th>Required level, service packs, patches</th>
<th>Supported partitioning technologies</th>
</tr>
</thead>
</table>
| 10 for IBM Power Systems (64-bit) | compat-libstdc++ (64-bit) Service Pack 1 for LPAR mobility | LPAR  
PowerVM - DLPAR  
PowerVM - Single Shared Processor Pool  
PowerVM - Micro-Partitioning  
LPAR mobility (Live Partition Mobility)  
Processor Factory Deconfiguration |
| 10 for IBM System z (64-bit) on 64-bit hardware | compat-libstdc++ (64-bit) | LPAR  
z/VM |
| 9 for Intel/AMD x86 (64-bit) | Service pack 1 to support sub-capacity pricing on Power 5 compat-libstdc++ (32 and 64-bit) | VMware ESX 2.5 - Single Server, Server Farm, Mobility (VMware Vmotion)  
VMware ESX 3.0 - Single Server, Cluster, Mobility (VMware Vmotion)  
VMware ESX 3.5 - Single Server, Cluster, Mobility (VMware Vmotion)  
VMware ESXi 3.5 - Single Server, Cluster, Mobility (VMware Vmotion)  
VMware ESX 4 - Single Server, Cluster, Mobility (VMware Vmotion)  
VMware ESXi 4 - Single Server, Cluster, Mobility (VMware Vmotion)  
VMware ESX 4.1 - Single Server, Cluster, Mobility (VMware Vmotion)  
VMware ESXi 4.1 - Single Server, Cluster, Mobility (VMware Vmotion)  
VMware vSphere 5 - Single Server, Cluster, Mobility (VMware Vmotion)  
Fix Pack 2 VMware vSphere 5.1 - Single Server, Cluster, Mobility (VMware Vmotion)  
Fix Pack 2 VMware vSphere 5.5 - Single Server, Cluster, Mobility (VMware Vmotion)  
BIOS (SMBIOS 2.5 or higher) & Operating System boot core limit  
System scaling using Intel QuickPath Interconnect |
| 9 for Intel/AMD x86 (32-bit)  | VMware ESX 2.5 - Single Server, Server Farm, Mobility (VMware Vmotion)  
VMware ESX 3.0 - Single Server, Cluster, Mobility (VMware Vmotion)  
VMware ESX 3.5 - Single Server, Cluster, Mobility (VMware Vmotion)  
VMware ESXi 3.5 - Single Server, Cluster, Mobility (VMware Vmotion)  
VMware ESX 4 - Single Server, Cluster, Mobility (VMware Vmotion)  
VMware ESXi 4 - Single Server, Cluster, Mobility (VMware Vmotion)  
VMware ESX 4.1 - Single Server, Cluster, Mobility (VMware Vmotion)  
VMware ESXi 4.1 - Single Server, Cluster, Mobility (VMware Vmotion)  
VMware vSphere 5 - Single Server, Cluster, Mobility (VMware Vmotion)  
Fix Pack 2 VMware vSphere 5.1 - Single Server, Cluster, Mobility (VMware Vmotion)  
Fix Pack 2 VMware vSphere 5.5 - Single Server, Cluster, Mobility (VMware Vmotion)  
BIOS (SMBIOS 2.5 or higher) & Operating System boot core limit  
System scaling using Intel QuickPath Interconnect |
### Supported versions of Novell Linux Desktop

<table>
<thead>
<tr>
<th>Version</th>
<th>Required level, service packs, patches</th>
<th>Supported partitioning technologies</th>
</tr>
</thead>
<tbody>
<tr>
<td>9 for Intel/AMD x86 (64-bit)</td>
<td>compat-libstdc++ (32 and 64-bit)</td>
<td>VMware ESX 2.5 - Single Server, Server Farm, Mobility (VMware Vmotion) VMware ESX 3.0 - Single Server, Cluster, Mobility (VMware Vmotion) VMware ESX 3.5 - Single Server, Cluster, Mobility (VMware Vmotion) VMware ESXi 3.5 - Single Server, Cluster, Mobility (VMware Vmotion) VMware ESX 4 - Single Server, Cluster, Mobility (VMware Vmotion) VMware ESXi 4 - Single Server, Cluster, Mobility (VMware Vmotion) VMware ESX 4.1 - Single Server, Cluster, Mobility (VMware Vmotion) VMware ESXi 4.1 - Single Server, Cluster, Mobility (VMware Vmotion)</td>
</tr>
<tr>
<td>9 for Intel/AMD x86 (32-bit)</td>
<td>compat-libstdc++ (32 and 64-bit)</td>
<td>VMware ESX 2.5 - Single Server, Server Farm, Mobility (VMware Vmotion) VMware ESX 3.0 - Single Server, Cluster, Mobility (VMware Vmotion) VMware ESX 3.5 - Single Server, Cluster, Mobility (VMware Vmotion) VMware ESXi 3.5 - Single Server, Cluster, Mobility (VMware Vmotion) VMware ESX 4 - Single Server, Cluster, Mobility (VMware Vmotion) VMware ESXi 4 - Single Server, Cluster, Mobility (VMware Vmotion) VMware ESX 4.1 - Single Server, Cluster, Mobility (VMware Vmotion) VMware ESXi 4.1 - Single Server, Cluster, Mobility (VMware Vmotion)</td>
</tr>
</tbody>
</table>

### Supported versions of Oracle Solaris

**Important:** If you are installing agents on a Solaris platform that is partitioned using the Containers partitioning technology, the HostID of the local zone must be the same as the HostID of the global zone.

<table>
<thead>
<tr>
<th>Version</th>
<th>Required level, service packs, patches</th>
<th>Supported partitioning technologies</th>
</tr>
</thead>
<tbody>
<tr>
<td>11 Operating System for x86 (64-bit)</td>
<td></td>
<td>Containers/Zones BIOS (SMBIOS 2.5 or higher) &amp; Operating System boot core limit</td>
</tr>
<tr>
<td>11 Operating System for SPARC (64-bit)</td>
<td></td>
<td>Dynamic System Domains. Solaris in Dynamic System Domains is supported but not for full capacity. Full capacity PVU values will need to be adjusted upward manually for the number of activated cores on the server. Dynamic Domains. Solaris in Dynamic Domains is supported but not for full capacity. Full capacity PVU values will need to be adjusted upward manually for the number of activated cores on the server. Containers/Zones: inside Dynamic System Domains and Dynamic Domains Containers/Zones: node OS Logical Domains - LDOMs (Oracle VM Server for SPARC 2.0) Containers/Zones: inside Logical Domains</td>
</tr>
<tr>
<td>10 Operating System for x86 (64-bit)</td>
<td></td>
<td>Containers/Zones BIOS (SMBIOS 2.5 or higher) &amp; Operating System boot core limit</td>
</tr>
<tr>
<td>10 Operating System for SPARC and UltraSPARC (64-bit)</td>
<td></td>
<td>Dynamic System Domains. Solaris in Dynamic System Domains is supported but not for full capacity. Full capacity PVU values will need to be adjusted upward manually for the number of activated cores on the server. Containers/Zones: inside Dynamic System Domains Containers/Zones: node OS</td>
</tr>
<tr>
<td>9 Operating System for UltraSPARC (32-bit and 64-bit)</td>
<td>Patches: 113713-03</td>
<td>Dynamic System Domains. Solaris in Dynamic System Domains is supported but not for full capacity. Full capacity PVU values will need to be adjusted upward manually for the number of activated cores on the server.</td>
</tr>
<tr>
<td>8 Operating System for UltraSPARC (32-bit and 64-bit)</td>
<td></td>
<td>Dynamic System Domains. Solaris in Dynamic System Domains is supported but not for full capacity. Full capacity PVU values will need to be adjusted upward manually for the number of activated cores on the server.</td>
</tr>
</tbody>
</table>
### Supported versions of Windows

<table>
<thead>
<tr>
<th>Version</th>
<th>Required level, service packs, patches</th>
<th>Supported partitioning technologies</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fix Pack 2</td>
<td>Fix Pack 2 Interim Fix 7</td>
<td>VMware vSphere 5 - Single Server, Cluster, Mobility (VMware Vmotion)</td>
</tr>
<tr>
<td>8.1 Enterprise</td>
<td>Fix Pack 2 Interim Fix 7</td>
<td>VMware vSphere 5.1 - Single Server, Cluster, Mobility (VMware Vmotion)</td>
</tr>
<tr>
<td>Fix Pack 2</td>
<td>Fix Pack 2 Interim Fix 7</td>
<td>VMware vSphere 5.5 - Single Server, Cluster, Mobility (VMware Vmotion)</td>
</tr>
<tr>
<td>8.1 Professional</td>
<td>Fix Pack 2 Interim Fix 7</td>
<td>Microsoft Hyper-V Server 2008 R2</td>
</tr>
<tr>
<td>Fix Pack 2</td>
<td>Fix Pack 2 Interim Fix 7</td>
<td>Microsoft Windows Server 2008 R2 with Hyper-V Role</td>
</tr>
<tr>
<td>8 Professional (32-bit and 64-bit)</td>
<td>Fix Pack 2 Interim Fix 7</td>
<td>Microsoft Windows Server 2008 R2 Hyper-V</td>
</tr>
<tr>
<td>Fix Pack 2</td>
<td>Fix Pack 2 Interim Fix 7</td>
<td>Microsoft Hyper-V Server 2012</td>
</tr>
<tr>
<td>7, including The United States Government Configuration Baseline (USGCB)</td>
<td>Fix Pack 2 Interim Fix 7</td>
<td>BIOS (SMBIOS 2.5 or higher) &amp; Operating System boot core limit</td>
</tr>
<tr>
<td>Fix Pack 2</td>
<td>Fix Pack 2 Interim Fix 7</td>
<td>System scaling using Intel QuickPath Interconnect</td>
</tr>
<tr>
<td>Vista Ultimate (32-bit and 64-bit)</td>
<td>Service Pack 2 for Microsoft Hyper-V Server 2012</td>
<td>VMware ESX 3.0 - Single Server, Cluster, Mobility (VMware Vmotion)</td>
</tr>
<tr>
<td>Fix Pack 2</td>
<td>Fix Pack 2 Interim Fix 7</td>
<td>VMware ESX 3.5 - Single Server, Cluster, Mobility (VMware Vmotion)</td>
</tr>
<tr>
<td>Fix Pack 2</td>
<td>Fix Pack 2 Interim Fix 7</td>
<td>VMware ESXi 4 - Single Server, Cluster, Mobility (VMware Vmotion)</td>
</tr>
<tr>
<td>Fix Pack 2</td>
<td>Fix Pack 2 Interim Fix 7</td>
<td>VMware ESXi 4.1 - Single Server, Cluster, Mobility (VMware Vmotion)</td>
</tr>
<tr>
<td>Fix Pack 2</td>
<td>Fix Pack 2 Interim Fix 7</td>
<td>VMware vSphere 5 - Single Server, Cluster, Mobility (VMware Vmotion)</td>
</tr>
<tr>
<td>Fix Pack 2</td>
<td>Fix Pack 2 Interim Fix 7</td>
<td>VMware vSphere 5.1 - Single Server, Cluster, Mobility (VMware Vmotion)</td>
</tr>
<tr>
<td>Fix Pack 2</td>
<td>Fix Pack 2 Interim Fix 7</td>
<td>VMware vSphere 5.5 - Single Server, Cluster, Mobility (VMware Vmotion)</td>
</tr>
<tr>
<td>Fix Pack 2</td>
<td>Fix Pack 2 Interim Fix 7</td>
<td>Microsoft Hyper-V 2008</td>
</tr>
<tr>
<td>Fix Pack 2</td>
<td>Fix Pack 2 Interim Fix 7</td>
<td>Microsoft Hyper-V Server 2008 R2</td>
</tr>
<tr>
<td>Fix Pack 2</td>
<td>Fix Pack 2 Interim Fix 7</td>
<td>Microsoft Hyper-V Server 2012</td>
</tr>
<tr>
<td>Fix Pack 2</td>
<td>Fix Pack 2 Interim Fix 7</td>
<td>Microsoft Windows Server 2008 R2 with Hyper-V Role</td>
</tr>
<tr>
<td>Fix Pack 2</td>
<td>Fix Pack 2 Interim Fix 7</td>
<td>Microsoft Windows Server 2008 R2 Hyper-V</td>
</tr>
<tr>
<td>Fix Pack 2</td>
<td>Fix Pack 2 Interim Fix 7</td>
<td>BIOS (SMBIOS 2.5 or higher) &amp; Operating System boot core limit</td>
</tr>
<tr>
<td>Fix Pack 2</td>
<td>Fix Pack 2 Interim Fix 7</td>
<td>System scaling using Intel QuickPath Interconnect</td>
</tr>
<tr>
<td>Version</td>
<td>Required level, service packs, patches</td>
<td>Supported partitioning technologies</td>
</tr>
<tr>
<td>---------------------------------</td>
<td>---------------------------------------</td>
<td>-------------------------------------</td>
</tr>
</tbody>
</table>
| **Vista Enterprise**            | Service Pack 2 for Microsoft Hyper-V Server 2012 | VMware ESX 3.0 - Single Server, Cluster, Mobility (VMware Vmotion)  
VMware ESX 3.5 - Single Server, Cluster, Mobility (VMware Vmotion)  
VMware ESXi 3.5 - Single Server, Cluster, Mobility (VMware Vmotion)  
VMware ESX 4 - Single Server, Cluster, Mobility (VMware Vmotion)  
VMware ESXi 4 - Single Server, Cluster, Mobility (VMware Vmotion)  
VMware ESX 4.1 - Single Server, Cluster, Mobility (VMware Vmotion)  
VMware ESXi 4.1 - Single Server, Cluster, Mobility (VMware Vmotion)  
VMware vSphere 5 - Single Server, Cluster, Mobility (VMware Vmotion)  
**Fix Pack 2** VMware vSphere 5.1 - Single Server, Cluster, Mobility (VMware Vmotion)  
**Fix Pack 2** VMware vSphere 5.5 - Single Server, Cluster, Mobility (VMware Vmotion)  
Microsoft Hyper-V 2008  
Microsoft Hyper-V Server 2008 R2  
Microsoft Hyper-V Server 2012  
Microsoft Windows Server 2008 R2 with Hyper-V Role  
Microsoft Windows Server 2008 R2 Hyper-V  
BIOS (SMBIOS 2.5 or higher) & Operating System boot core limit  
System scaling using Intel QuickPath Interconnect |
| **Vista Business**              | Service Pack 2 for Microsoft Hyper-V Server 2012 | VMware ESX 3.0 - Single Server, Cluster, Mobility (VMware Vmotion)  
VMware ESX 3.5 - Single Server, Cluster, Mobility (VMware Vmotion)  
VMware ESXi 3.5 - Single Server, Cluster, Mobility (VMware Vmotion)  
VMware ESX 4 - Single Server, Cluster, Mobility (VMware Vmotion)  
VMware ESXi 4 - Single Server, Cluster, Mobility (VMware Vmotion)  
VMware ESX 4.1 - Single Server, Cluster, Mobility (VMware Vmotion)  
VMware ESXi 4.1 - Single Server, Cluster, Mobility (VMware Vmotion)  
VMware vSphere 5 - Single Server, Cluster, Mobility (VMware Vmotion)  
**Fix Pack 2** VMware vSphere 5.1 - Single Server, Cluster, Mobility (VMware Vmotion)  
**Fix Pack 2** VMware vSphere 5.5 - Single Server, Cluster, Mobility (VMware Vmotion)  
Microsoft Hyper-V 2008  
Microsoft Hyper-V Server 2008 R2  
Microsoft Hyper-V Server 2012  
Microsoft Windows Server 2008 R2 with Hyper-V Role  
Microsoft Windows Server 2008 R2 Hyper-V  
BIOS (SMBIOS 2.5 or higher) & Operating System boot core limit  
System scaling using Intel QuickPath Interconnect |
| **Fix Pack 2** **Interim Fix 7** | **Server 2012 R2 Standard and Datacenter** | VMware vSphere 5 - Single Server, Cluster, Mobility (VMware Vmotion)  
**Fix Pack 2** **Interim Fix 7** VMware vSphere 5.1 - Single Server, Cluster, Mobility (VMware Vmotion)  
**Fix Pack 2** **Interim Fix 7** VMware vSphere 5.5 - Single Server, Cluster, Mobility (VMware Vmotion)  
**Fix Pack 2** **Interim Fix 7** Microsoft Hyper-V Server 2008 R2  
**Fix Pack 2** **Interim Fix 7** Microsoft Windows Server 2008 R2 Hyper-V Role  
**Fix Pack 2** **Interim Fix 7** Microsoft Windows Server 2008 R2 Hyper-V  
**Fix Pack 2** **Interim Fix 7** Microsoft Hyper-V Server 2012  
**Fix Pack 2** **Interim Fix 7** BIOS (SMBIOS 2.5 or higher) & Operating System boot core limit  
**Fix Pack 2** **Interim Fix 7** System scaling using Intel QuickPath Interconnect |
<table>
<thead>
<tr>
<th>Version</th>
<th>Required level, service packs, patches</th>
<th>Supported partitioning technologies</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server 2008 R2 Standard, Enterprise, and Datacenter (64-bit) for Intel x86</td>
<td>VMware ESX 3.5 - Single Server, Cluster, Mobility (VMware Vmotion) VMware ESXi 3.5 - Single Server, Cluster, Mobility (VMware Vmotion) VMware ESX 4 - Single Server, Cluster, Mobility (VMware Vmotion) VMware ESXi 4 - Single Server, Cluster, Mobility (VMware Vmotion) VMware ESX 4.1 - Single Server, Cluster, Mobility (VMware Vmotion) VMware ESXi 4.1 - Single Server, Cluster, Mobility (VMware Vmotion) VMware vSphere 5 - Single Server, Cluster, Mobility (VMware Vmotion) Fix Pack 2 VMware vSphere 5.1 - Single Server, Cluster, Mobility (VMware Vmotion) Fix Pack 2 VMware vSphere 5.5 - Single Server, Cluster, Mobility (VMware Vmotion) Microsoft Hyper-V 2008 Microsoft Hyper-V Server 2008 R2 Microsoft Hyper-V Server 2012 Microsoft Windows Server 2008 R2 with Hyper-V Role Microsoft Windows Server 2008 R2 Hyper-V BIOS (SMBIOS 2.5 or higher) &amp; Operating System boot core limit System scaling using Intel QuickPath Interconnect</td>
<td></td>
</tr>
<tr>
<td>Server 2008 Standard and Enterprise (32-bit and 64-bit) for Intel x86</td>
<td>VMware ESX 3.5 - Single Server, Cluster, Mobility (VMware Vmotion) VMware ESXi 3.5 - Single Server, Cluster, Mobility (VMware Vmotion) VMware ESX 4 - Single Server, Cluster, Mobility (VMware Vmotion) VMware ESXi 4 - Single Server, Cluster, Mobility (VMware Vmotion) VMware ESX 4.1 - Single Server, Cluster, Mobility (VMware Vmotion) VMware ESXi 4.1 - Single Server, Cluster, Mobility (VMware Vmotion) VMware vSphere 5 - Single Server, Cluster, Mobility (VMware Vmotion) Fix Pack 2 VMware vSphere 5.1 - Single Server, Cluster, Mobility (VMware Vmotion) Fix Pack 2 VMware vSphere 5.5 - Single Server, Cluster, Mobility (VMware Vmotion) Microsoft Hyper-V 2008 Microsoft Hyper-V Server 2008 R2 Microsoft Hyper-V Server 2012 Microsoft Windows Server 2008 R2 with Hyper-V Role Microsoft Windows Server 2008 R2 Hyper-V BIOS (SMBIOS 2.5 or higher) &amp; Operating System boot core limit System scaling using Intel QuickPath Interconnect</td>
<td></td>
</tr>
<tr>
<td>Server 2003 R2 (32-bit and 64-bit)</td>
<td>Service Pack 2</td>
<td>VMware ESX 2.5 - Single Server, Server Farm, Mobility (VMware Vmotion) VMware ESX 3.0 - Single Server, Cluster, Mobility (VMware Vmotion) VMware ESX 3.5 - Single Server, Cluster, Mobility (VMware Vmotion) VMware ESXi 3.5 - Single Server, Cluster, Mobility (VMware Vmotion) VMware ESX 4 - Single Server, Cluster, Mobility (VMware Vmotion) VMware ESXi 4 - Single Server, Cluster, Mobility (VMware Vmotion) VMware ESX 4.1 - Single Server, Cluster, Mobility (VMware Vmotion) VMware ESXi 4.1 - Single Server, Cluster, Mobility (VMware Vmotion) VMware vSphere 5 - Single Server, Cluster, Mobility (VMware Vmotion) Fix Pack 2 VMware vSphere 5.1 - Single Server, Cluster, Mobility (VMware Vmotion) Fix Pack 2 VMware vSphere 5.5 - Single Server, Cluster, Mobility (VMware Vmotion) Microsoft Hyper-V 2008 Microsoft Hyper-V Server 2008 R2 Microsoft Hyper-V Server 2012 Microsoft Windows Server 2008 R2 with Hyper-V Role Microsoft Windows Server 2008 R2 Hyper-V BIOS (SMBIOS 2.5 or higher) &amp; Operating System boot core limit (with the exception of XP) System scaling using Intel QuickPath Interconnect</td>
</tr>
<tr>
<td>Version</td>
<td>Required level, service packs, patches</td>
<td>Supported partitioning technologies</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>----------------------------------------</td>
<td>-------------------------------------</td>
</tr>
</tbody>
</table>
| Server 2003 Standard Edition (32-bit and 64-bit) | Service Pack 2                           | VMware ESX 2.5 - Single Server, Server Farm, Mobility (VMware Vmotion)  
VMware ESX 3.0 - Single Server, Cluster, Mobility (VMware Vmotion)  
VMware ESX 3.5 - Single Server, Cluster, Mobility (VMware Vmotion)  
VMware ESXi 3.5 - Single Server, Cluster, Mobility (VMware Vmotion)  
VMware ESX 4 - Single Server, Cluster, Mobility (VMware Vmotion)  
VMware ESXi 4 - Single Server, Cluster, Mobility (VMware Vmotion)  
VMware ESX 4.1 - Single Server, Cluster, Mobility (VMware Vmotion)  
VMware ESXi 4.1 - Single Server, Cluster, Mobility (VMware Vmotion)  
VMware vSphere 5 - Single Server, Cluster, Mobility (VMware Vmotion)  
Fix Pack 2 VMware vSphere 5.1 - Single Server, Cluster, Mobility (VMware Vmotion)  
Fix Pack 2 VMware vSphere 5.5 - Single Server, Cluster, Mobility (VMware Vmotion)  
Microsoft Virtual Server 2005  
Microsoft Hyper-V 2008  
Microsoft Hyper-V Server 2008 R2  
Microsoft Hyper-V Server 2012  
Microsoft Windows Server 2008 R2 with Hyper-V Role  
Microsoft Windows Server 2008 R2 Hyper-V  
BIOS (SMBIOS 2.5 or higher) & Operating System boot core limit  
System scaling using Intel QuickPath Interconnect |
| Server 2003 Enterprise Edition (32-bit and 64-bit) | Service Pack 2                           | VMware vSphere 5.5 - Single Server, Cluster, Mobility (VMware Vmotion)  
Microsoft Virtual Server 2005  
Microsoft Hyper-V 2008  
Microsoft Hyper-V Server 2008 R2  
Microsoft Hyper-V Server 2012  
Microsoft Windows Server 2008 R2 with Hyper-V Role  
Microsoft Windows Server 2008 R2 Hyper-V  
BIOS (SMBIOS 2.5 or higher) & Operating System boot core limit  
System scaling using Intel QuickPath Interconnect |
| XP Professional               | Service Pack 2                           | VMware vSphere 5.5 - Single Server, Cluster, Mobility (VMware Vmotion)  
Microsoft Virtual Server 2005  
Microsoft Hyper-V 2008  
Microsoft Hyper-V Server 2008 R2  
Microsoft Hyper-V Server 2012  
Microsoft Windows Server 2008 R2 with Hyper-V Role  
Microsoft Windows Server 2008 R2 Hyper-V  
BIOS (SMBIOS 2.5 or higher) & Operating System boot core limit  
System scaling using Intel QuickPath Interconnect |

**VMware and Microsoft virtualization considerations**

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

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

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

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

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

- Microsoft Virtual Server
- VMware ESX Server 4.1
- VMware ESX Server 4.0
- VMware ESX Server 3.5
- VMware ESX Server 3.0
On VMware ESX Server 3.0 and 3.5, the enabler can also be run on partitions which are managed through a server using VMware Virtual Center. However, it is recommended to use the VM manager in those cases.

**Important:** You have to use VM managers in cluster environments to ensure that the virtual machine hierarchy is built correctly. Note that in such situations, you should not use Common Inventory Technology enabler because it cannot provide complete information about cluster topology.

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

### Other software requirements for the agents

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

### Software corequisites for agents

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

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

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

<table>
<thead>
<tr>
<th>Operating System</th>
<th>Version</th>
<th>Global Security Toolkit Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>IBM i</td>
<td>V5R3, V5R4, V6R1</td>
<td>6b</td>
</tr>
<tr>
<td>Other platforms</td>
<td></td>
<td>7.0.4.14</td>
</tr>
</tbody>
</table>

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

Common Inventory Technology enabler is a script that enables the Common Inventory Technology to obtain information about partitioned environments. It is required by the agent on systems not managed by VM managers such as ESX (3.0, 3.5, 4.0, 4.1) or Virtual Center.
Table 23. Common Inventory Technology enabler

<table>
<thead>
<tr>
<th>Partitioning technology</th>
<th>Platform</th>
<th>Files</th>
<th>Subdirectory</th>
</tr>
</thead>
<tbody>
<tr>
<td>VMWare</td>
<td>Windows</td>
<td>cpuid.exe</td>
<td>enabler\VMWare\w32-ix86</td>
</tr>
<tr>
<td></td>
<td></td>
<td>wenvmw.exe</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>retrieve.pl</td>
<td></td>
</tr>
<tr>
<td>Linux</td>
<td></td>
<td>cpuid.exe</td>
<td>enabler\VMWare\linux-ix86</td>
</tr>
<tr>
<td></td>
<td></td>
<td>wenvmw.sh</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>retrieve.pl</td>
<td></td>
</tr>
<tr>
<td>Microsoft Virtual Server</td>
<td>Windows</td>
<td>cpuid.exe</td>
<td>enabler\MSVirtualServer</td>
</tr>
<tr>
<td></td>
<td></td>
<td>wenvmsvs.exe</td>
<td></td>
</tr>
</tbody>
</table>

Tools required to install the agent on a virtual machine

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

Table 24. Partitioning technology prerequisites

<table>
<thead>
<tr>
<th>Partitioning technology</th>
<th>Tool</th>
</tr>
</thead>
<tbody>
<tr>
<td>VMware ESX 2.5</td>
<td>VMware Tools - optional.</td>
</tr>
<tr>
<td>VMware ESX 3.0</td>
<td>If you do not use VM manager to augment the data reported by agents, they will be in 'Incomplete' state and will report the wrong topology and measures.</td>
</tr>
<tr>
<td>VMware ESX 3.5</td>
<td></td>
</tr>
<tr>
<td>VMware ESXi 3.5</td>
<td></td>
</tr>
<tr>
<td>VMware ESX 4</td>
<td></td>
</tr>
<tr>
<td>VMware ESXi 4</td>
<td></td>
</tr>
<tr>
<td>Microsoft Virtual Server 2005</td>
<td>Microsoft Virtual Machine Additions</td>
</tr>
<tr>
<td>HP Integrity Virtual Machines</td>
<td>Host operating system</td>
</tr>
<tr>
<td></td>
<td>HPVM package</td>
</tr>
<tr>
<td></td>
<td>Guest operating system</td>
</tr>
<tr>
<td></td>
<td>HPVM-Guest</td>
</tr>
</tbody>
</table>

The installation of the lsvpd utility on Power5+ QCM processors


After the installation of the lsvpd utility, you need to initialize the database by issuing the following command: `/etc/init.d/lsvpd start`

sed and grep

Sed and grep binary files are required on computers on which agents are to be installed. These binaries are needed during the installation of agents.
Windows Management Instrumentation

Windows Management Instrumentation must be enabled on Windows computers in order to run the agent.

Disk space requirements

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

For all agent deployment methods, a space check is made to ensure that the installation will not start and then fail because of lack of sufficient space in the agent installation directory. If the space available is insufficient, the installation fails with a message that the agent signature file could not be written to the agent installation folder.

Agent space requirements for AIX

<table>
<thead>
<tr>
<th>Operating system</th>
<th>Directory</th>
<th>Directory</th>
<th>Space required</th>
</tr>
</thead>
<tbody>
<tr>
<td>AIX, 7.2.2 GA installation package</td>
<td>Agent installation directory (default: /var/itlm)</td>
<td>55 MB</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Temporary directory (default: /tmp)</td>
<td>70 MB</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Tivoli_Common_Directory/COD</td>
<td>10 MB</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Directory for configuration files (default: /etc)</td>
<td>under 1 MB</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Common Inventory Technology (default directory: /opt/tivoli/cit)</td>
<td>40 MB</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Common Inventory Technology cache files (default: /opt/tivoli/cit/cache_data/__username)</td>
<td>about 500 MB</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Depends on the number of files, directories, and subdirectories to be scanned. Can be estimated by multiplying the number of files to be scanned by 60 bytes.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>AIX, 7.2.2 fix pack 1 installation package, and standard installation location</td>
<td>Agent application directory (default: /opt/itlm)</td>
<td>26 MB</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Agent data directory (/var/itlm)</td>
<td>29 MB</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Temporary directory (default: /tmp)</td>
<td>70 MB</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Tivoli_Common_Directory/COD</td>
<td>10 MB</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Directory for configuration files (default: /etc)</td>
<td>under 1 MB</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Common Inventory Technology (default directory: /opt/tivoli/cit)</td>
<td>40 MB</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Common Inventory Technology cache files (default: /opt/tivoli/cit/cache_data/__username)</td>
<td>about 500 MB</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Depends on the number of files, directories, and subdirectories to be scanned. Can be estimated by multiplying the number of files to be scanned by 60 bytes.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Table 25. Tivoli Asset Discovery for Distributed agent space requirements (continued)

<table>
<thead>
<tr>
<th>AIX using 7.2.2 fix pack 1 installation package, and non-standard installation location</th>
<th>Agent installation directory - User Specified Installation Location (USIL) created with mkusil command</th>
<th>58 MB</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Temporary directory (default: /tmp)</td>
<td>70 MB</td>
</tr>
<tr>
<td></td>
<td>Tivoli_Common_Directory/COD</td>
<td>10 MB</td>
</tr>
<tr>
<td></td>
<td>Directory for configuration files (default: /etc)</td>
<td>under 1 MB</td>
</tr>
<tr>
<td></td>
<td>Common Inventory Technology (default directory: /opt/tivoli/cit)</td>
<td>40 MB</td>
</tr>
<tr>
<td></td>
<td>Common Inventory Technology cache files (default: /opt/tivoli/cit/cache_data/__username)</td>
<td>about 500 MB</td>
</tr>
<tr>
<td></td>
<td>Depends on the number of files, directories, and subdirectories to be scanned. Can be estimated by multiplying the number of files to be scanned by 60 bytes.</td>
<td></td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Operating system</th>
<th>Directory</th>
<th>Space required</th>
</tr>
</thead>
<tbody>
<tr>
<td>HP-UX on PA-RISC</td>
<td>Agent installation directory (default: /var/itm)</td>
<td>100 MB</td>
</tr>
<tr>
<td></td>
<td>Temporary directory (default: /tmp)</td>
<td>90 MB</td>
</tr>
<tr>
<td></td>
<td>Tivoli_Common_Directory/COD</td>
<td>10 MB</td>
</tr>
<tr>
<td></td>
<td>Directory for configuration files (default: /etc)</td>
<td>under 1 MB</td>
</tr>
<tr>
<td></td>
<td>Common Inventory Technology (default directory: /opt/tivoli/cit)</td>
<td>30 MB</td>
</tr>
<tr>
<td></td>
<td>Common Inventory Technology cache files (default: /opt/tivoli/cit/cache_data/__username)</td>
<td>about 500 MB</td>
</tr>
<tr>
<td></td>
<td>Depends on the number of files, directories, and subdirectories to be scanned. Can be estimated by multiplying the number of files to be scanned by 60 bytes.</td>
<td></td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Operating system</th>
<th>Directory</th>
<th>Space required</th>
</tr>
</thead>
<tbody>
<tr>
<td>HP-UX on Itanium 2 Integrity Server</td>
<td>Agent installation directory (default: /var/itm)</td>
<td>130 MB</td>
</tr>
<tr>
<td></td>
<td>Temporary directory (default: /tmp)</td>
<td>120 MB</td>
</tr>
<tr>
<td></td>
<td>Tivoli_Common_Directory/COD</td>
<td>10 MB</td>
</tr>
<tr>
<td></td>
<td>Directory for configuration files (default: /etc)</td>
<td>under 1 MB</td>
</tr>
<tr>
<td></td>
<td>Common Inventory Technology (default directory: /opt/tivoli/cit)</td>
<td>50 MB</td>
</tr>
<tr>
<td></td>
<td>Common Inventory Technology cache files (default: /opt/tivoli/cit/cache_data/__username)</td>
<td>about 500 MB</td>
</tr>
<tr>
<td></td>
<td>Depends on the number of files, directories, and subdirectories to be scanned. Can be estimated by multiplying the number of files to be scanned by 60 bytes.</td>
<td></td>
</tr>
</tbody>
</table>
### Agent space requirements for IBM i

<table>
<thead>
<tr>
<th>Operating system</th>
<th>Directory</th>
<th>Space required</th>
</tr>
</thead>
<tbody>
<tr>
<td>IBM i (formerly i5/OS™)</td>
<td>Agent installation directory</td>
<td>80 MB</td>
</tr>
<tr>
<td></td>
<td>Temporary directory (default: /tmp)</td>
<td>130 MB</td>
</tr>
<tr>
<td></td>
<td>Tivoli_Common_Directory/COD</td>
<td>10 MB</td>
</tr>
<tr>
<td></td>
<td>Common Inventory Technology (default directory: /opt/tivoli/cit)</td>
<td>55 MB</td>
</tr>
<tr>
<td></td>
<td>Common Inventory Technology cache files (default: /opt/tivoli/cit/cache_data/__username)</td>
<td>about 500 MB</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Depends on the number of files, directories, and subdirectories to be scanned. Can be estimated by multiplying the number of files to be scanned by 60 bytes.</td>
</tr>
</tbody>
</table>

### Agent space requirements for Linux x86

<table>
<thead>
<tr>
<th>Operating system</th>
<th>Directory</th>
<th>Space required</th>
</tr>
</thead>
<tbody>
<tr>
<td>Linux x86</td>
<td>Agent installation directory (default: /var/itm)</td>
<td>40 MB</td>
</tr>
<tr>
<td></td>
<td>Temporary directory (default: /tmp)</td>
<td>50 MB</td>
</tr>
<tr>
<td></td>
<td>Tivoli_Common_Directory/COD</td>
<td>10 MB</td>
</tr>
<tr>
<td></td>
<td>Directory for configuration files (default: /etc)</td>
<td>under 1 MB</td>
</tr>
<tr>
<td></td>
<td>Common Inventory Technology</td>
<td>30 MB</td>
</tr>
<tr>
<td></td>
<td>Common Inventory Technology cache files (default: /opt/tivoli/cit/cache_data/__username)</td>
<td>about 500 MB</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Depends on the number of files, directories, and subdirectories to be scanned. Can be estimated by multiplying the number of files to be scanned by 60 bytes.</td>
</tr>
</tbody>
</table>

### Agent space requirements for Linux pSeries

<table>
<thead>
<tr>
<th>Operating system</th>
<th>Directory</th>
<th>Space required</th>
</tr>
</thead>
<tbody>
<tr>
<td>Linux on Power Systems</td>
<td>Agent installation directory (default: /var/itm)</td>
<td>40 MB</td>
</tr>
<tr>
<td></td>
<td>Temporary directory (default: /tmp)</td>
<td>50 MB</td>
</tr>
<tr>
<td></td>
<td>Tivoli_Common_Directory/COD</td>
<td>10 MB</td>
</tr>
<tr>
<td></td>
<td>Directory for configuration files (default: /etc)</td>
<td>under 1 MB</td>
</tr>
<tr>
<td></td>
<td>Common Inventory Technology</td>
<td>30 MB</td>
</tr>
<tr>
<td></td>
<td>Common Inventory Technology cache files (default: /opt/tivoli/cit/cache_data/__username)</td>
<td>about 500 MB</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Depends on the number of files, directories, and subdirectories to be scanned. Can be estimated by multiplying the number of files to be scanned by 60 bytes.</td>
</tr>
</tbody>
</table>
### Agent space requirements for Linux zSeries

<table>
<thead>
<tr>
<th>Operating system</th>
<th>Directory</th>
<th>Space required</th>
</tr>
</thead>
<tbody>
<tr>
<td>Linux on System z</td>
<td>Agent installation directory (default: /var/itm)</td>
<td>100 MB</td>
</tr>
<tr>
<td></td>
<td>Temporary directory (default: /tmp)</td>
<td>60 MB</td>
</tr>
<tr>
<td></td>
<td>Tivoli_Common_Directory/COD</td>
<td>10 MB</td>
</tr>
<tr>
<td></td>
<td>Directory for configuration files (default: /etc)</td>
<td>under 1 MB</td>
</tr>
<tr>
<td></td>
<td>Common Inventory Technology</td>
<td>30 MB</td>
</tr>
<tr>
<td></td>
<td>Common Inventory Technology cache files (default: /opt/tivoli/cit/cache_data/__username)</td>
<td>about 500 MB</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Depends on the number of files, directories, and subdirectories to be scanned. Can be estimated by multiplying the number of files to be scanned by 60 bytes.</td>
</tr>
</tbody>
</table>

### Agent space requirements for Solaris on x86

<table>
<thead>
<tr>
<th>Operating system</th>
<th>Directory</th>
<th>Space required</th>
</tr>
</thead>
<tbody>
<tr>
<td>Solaris on x86</td>
<td>Agent installation directory (default: /var/itm)</td>
<td>50 MB</td>
</tr>
<tr>
<td></td>
<td>Temporary directory (default: /tmp)</td>
<td>55 MB</td>
</tr>
<tr>
<td></td>
<td>Tivoli_Common_Directory/COD</td>
<td>10 MB</td>
</tr>
<tr>
<td></td>
<td>Directory for configuration files (default: /etc)</td>
<td>under 1 MB</td>
</tr>
<tr>
<td></td>
<td>Common Inventory Technology (default directory: /opt/tivoli/cit)</td>
<td>25 MB</td>
</tr>
<tr>
<td></td>
<td>Common Inventory Technology cache files (default: /opt/tivoli/cit/cache_data/__username)</td>
<td>about 500 MB</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Depends on the number of files, directories, and subdirectories to be scanned. Can be estimated by multiplying the number of files to be scanned by 60 bytes.</td>
</tr>
</tbody>
</table>

### Agent space requirements for Solaris on SPARC

<table>
<thead>
<tr>
<th>Operating system</th>
<th>Directory</th>
<th>Space required</th>
</tr>
</thead>
<tbody>
<tr>
<td>Solaris on SPARC</td>
<td>Agent installation directory (default: /var/itm)</td>
<td>55 MB</td>
</tr>
<tr>
<td></td>
<td>Temporary directory (default: /tmp)</td>
<td>65 MB</td>
</tr>
<tr>
<td></td>
<td>Tivoli_Common_Directory/COD</td>
<td>10 MB</td>
</tr>
<tr>
<td></td>
<td>Directory for configuration files (default: /etc)</td>
<td>under 1 MB</td>
</tr>
<tr>
<td></td>
<td>Common Inventory Technology (default directory: /opt/tivoli/cit)</td>
<td>25 MB</td>
</tr>
<tr>
<td></td>
<td>Common Inventory Technology cache files (default: /opt/tivoli/cit/cache_data/__username)</td>
<td>about 500 MB</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Depends on the number of files, directories, and subdirectories to be scanned. Can be estimated by multiplying the number of files to be scanned by 60 bytes.</td>
</tr>
</tbody>
</table>
### Agent space requirements for Windows

<table>
<thead>
<tr>
<th>Operating system</th>
<th>Directory</th>
<th>Space required</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows</td>
<td>Agent installation directory (default: %WINDIR%/itm).</td>
<td>35 MB</td>
</tr>
<tr>
<td></td>
<td>Temporary directory (default: %TEMP%)</td>
<td>30 MB</td>
</tr>
<tr>
<td></td>
<td>Tivoli_Common_Directory/COD</td>
<td>10 MB</td>
</tr>
<tr>
<td></td>
<td>Directory for configuration files (default: %WINDIR%)</td>
<td>under 1 MB</td>
</tr>
<tr>
<td></td>
<td>Common Inventory Technology (default directory: C:\Program Files\tivoli\cit)</td>
<td>10 MB</td>
</tr>
<tr>
<td></td>
<td>Common Inventory Technology cache files (default: /opt/tivoli/cit/cache_data/__username)</td>
<td>about 500 MB</td>
</tr>
</tbody>
</table>

Depends on the number of files, directories, and subdirectories to be scanned. Can be estimated by multiplying the number of files to be scanned by 60 bytes.

### Support for high availability environments

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

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

The following scenarios have been validated:

**High Availability Cluster Multiprocessing configurations**
- Hot StandBy
- Mutual Takeover
- Concurrent Access with or without IBM General Parallel File System

**High Availability Cluster Multiprocessing Policy**
- Rotating

**Tivoli Asset Discovery for Distributed configuration**

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

**Applications**

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

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

IBM Tivoli Asset Discovery for Distributed provides support for system scaling using Intel QuickPath Interconnect that enables scalable PVU consumption. The support has been introduced with Fix Pack 1 for Tivoli Asset Discovery for Distributed 7.2.2.

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

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

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

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

<table>
<thead>
<tr>
<th>Day 1: the computers are separated</th>
<th>Day 2, 10 a.m.: computer B is connected to computer A with the QuickPath Interconnect link</th>
</tr>
</thead>
</table>
| Computer A:  
• 2 sockets  
• 8 cores  
• 70 PVU per core  
• 1 agent with DB2 and WebSphere Application Server installed | Computer B:  
• 2 sockets  
• 8 cores  
• 70 PVU per core  
• 1 agent with DB2 installed |
| Computer A:  
• 4 sockets  
• 16 cores  
• 100 PVU per core  
• 1 agent with DB2 and WebSphere Application Server installed | Computer B:  
Offline from 10 a.m. |

The report generated for day 2 lists the following items:  
• DB2: 24 cores  
• WebSphere Application Server: 16 cores

There is no technical possibility to automatically detect the problem and exclude computer B from the report for day 2. The situation might result in overcharging. To prevent the problem, you can either disable the agent the day before you connect the computers (UTC time), or exclude the miscalculated product instances on the agent on computer B from the report.
To disable the agent:
1. Shut down or uninstall the agent on computer B one day before the connection date.
2. Remove the agent from the Tivoli Asset Discovery for Distributed Web user interface.
3. Connect the computers the next day.

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

**Supported national languages for IBM i agents**

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

<table>
<thead>
<tr>
<th>Installed languages on IBM i</th>
</tr>
</thead>
<tbody>
<tr>
<td>Language code</td>
</tr>
<tr>
<td>2924</td>
</tr>
<tr>
<td>2928</td>
</tr>
<tr>
<td>2929</td>
</tr>
<tr>
<td>2931</td>
</tr>
<tr>
<td>2932</td>
</tr>
<tr>
<td>2962</td>
</tr>
<tr>
<td>2975</td>
</tr>
<tr>
<td>2976</td>
</tr>
<tr>
<td>2978</td>
</tr>
<tr>
<td>2979</td>
</tr>
<tr>
<td>2980</td>
</tr>
<tr>
<td>2986</td>
</tr>
<tr>
<td>2987</td>
</tr>
<tr>
<td>2989</td>
</tr>
</tbody>
</table>

**Agent preinstallation steps**

Depending on your software and the security level you selected, there are several tasks you need to perform before you install the agents. For example, if you are going to use secure communications, you must enable a valid certificate for the server and agents.

In order to install agents you need to have root (UNIX) or Administrator (Windows) authority. This is because each agent is registered as system service.

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

**Important:**
The agent installer does not allow you to use non-Latin characters when specifying path names (such as the agent installation path, Common Inventory Technology installation path or the temporary folder for the agent), and the scan group name. If you need to add the agent to a scan group that has non-Latin characters in its name, add it to a different group at installation time, then reassign it to the target scan group after the installation finishes.

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

To install and run agents, you must have root (UNIX) or Administrator (Windows) authority. This requirement is mandatory because each agent is registered as system service.

Procedure

1. Gather the following information:
   - Asset Discovery for Distributed server address and the port number that agents are to use.
   - Level of security that has been configured for the server. At the server command line, issue the command `getserverconf -k agentToServerSecurityLevel`
   - The proxy port and address if you want the agent to use a proxy server for communication with the server.

2. **Download and install the unrestricted JCE policy files** if you are planning to use secure communication between the agents and the administration server (medium or maximum security level).

3. Enable a valid certificate for the administration server (if you have defined medium or maximum security level while installing the server). To do that, perform the following steps:
   a. Create a certificate authority request
   b. Receive a certificate issued by a certificate authority
   c. Replace an existing certificate with the new one.
   You might also create a self-signed certificate or use the one installed with the server by default (not recommended for production environments).

4. **UNIX** If you want to install agents on a shared file system, ensure that you have exported and mounted the remote directory so as to allow changing permissions on mounted directories and files, for example `chown` and `chmod` command.

5. Configure any firewalls between the agent and server computers to allow the agent access to the server.

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

7. **Windows** If Windows Terminal Server is installed on the computer where you want to run the setup file, or you are accessing another computer using Windows Terminal Services, ensure that the computer is in install mode when the setup file is launched.
   a. Issue the command `change user /install` from a Windows command line to change into install mode manually.
   b. After running the setup file, return to execute mode by running `change user /execute`. 
8. If you are using your own tools to install agents in bulk on a large number of computers, ensure that the value in the `current_working_directory` (when possible) parameter is not set to `null` when running a new process on an endpoint.

9. If you are installing the agent in a partitioned environment using VMware or Microsoft Virtual Server virtualization technologies, ensure you have configured VM managers.

   If your machine cannot be connected to a VM manager and runs on ESX 3.5, 3.5, 4.0 or 4.1, run the Common Inventory Technology enabler.

   **Important:** If you are installing the agent on Windows 2000 in Hyper-V environment, ensure that you have configured the virtual machine to use only one virtual processor. For details of how to do this, visit [Microsoft TechNet](https://technet.microsoft.com).

10. **Red Hat** Set SELinux to disabled.

11. **AIX** To install the agent in a different directory than the default one:

    - (AIX version 5.4 or higher) Specify the `User Specified Installation Location` (USIL) location:
      ```
      mkusil -R /opt/ITLM_agent
      installp -R /opt/ITLM_agent -acgXd ILMT-TAD4D-agent-7.2.2-aix-ppc ILMT-TAD4D-agent
      ```
    - (AIX version 5.3 or lower) Set the following environment variable:
      ```
      export ILMT_INSTALL_PATH=PATH_TO_DESIRED_LOCATION
      ```

12. **Windows** Enable *Windows Management Instrumentation* on Windows computers in order to run the agent after the installation.

### Preparing agent certificates for client authentication

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

**Procedure**

1. Log on to the administration server computer as Administrator (for Windows platforms) or root (for UNIX platforms) and start the Tivoli Asset Discovery for Distributed command-line interface.

2. **Enable and configure server security**.

3. Depending on how many agents you plan to deploy with maximum security, issue the `generateAgentId` command to generate that number of unique agent IDs, output certificate signing requests (CSRs), and private keys.

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

4. For each CSR, use your own Public Key Infrastructure (PKI) to do the following steps:
   - Get the request signed by a certificate authority to form an agent certificate.
   - Produce a PKCS12 keystore (`agent_ID.p12`) file, protected by a password, that contains the agent certificate, the private key, and the CA certificate. Set the friendly name to `itlm agent certificate`.

---

96
- Import the certificate authority (CA) certificate to the Signer Certificate section of the ILMT truststore on the server.
- Copy the keystore file to the directory on the server.

5. From the Tivoli Asset Discovery for Distributed command-line interface, issue the `convertcertificate` command to convert the keystore file to a format supported by the security software used by the agent. For agents on Windows, Linux and UNIX platforms, the command converts the files found in the directory where you copied the keystore file to the CMS format (`agent_ID.kdb`) and stores them in the same directory. For agents on IBM i, the command converts the files to the keystore format and version that is supported by IBM i and stores them in the same directory.

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

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

   The `slmtest` password must be used.

### Running Prerequisite Scanner

Run IBM Tivoli Asset Discovery for Distributed Prerequisite Scanner to perform identification, checking, and verification of prerequisites for agents before their installation.

#### Before you begin


- **UNIX** `precheck_unix_build_number.tar`
- **Windows** `precheck_windows_build_number.zip`

Tivoli Asset Discovery for Distributed Prerequisite Scanner is a tool that scans for agents hardware and software prerequisites. It displays the results of the scan in the command-line interface and also saves the results to human-readable log file (`result.txt`) regardless of whether you set the `detail` parameter.

Prerequisite Scanner initially checks the operating system of the computer and verifies whether it is the correct version for the specified software. If it is a supported operating system, it continues the prerequisite scan and generates the results; otherwise, the scanner exits.

#### Procedure

1. Copy the `precheck_scripts.zip` file from the product DVD or package downloaded from Passport Advantage onto the hard disk drive of the computer that you want to scan.

2. Extract the `precheck_scripts.zip` to a directory, for example to `C:\precheck` (Windows) or `/tmp` (UNIX, Linux). Ensure that in the temporary directory there are the following subdirectories and files:

   - **Linux** `UNIX` `UNIX_Linux` (directory)
   - **Windows** `Windows` (directory)
3. Open a command-line interface and change to the directory where you have extracted the files.

4. Set the execution permission rights for the TAD.sh script file.

5. Supply the values for the parameters in the appropriate file (depending on the platform):
   - PATH: Product installation path
   - SERVER: Administration server IP address
   - TAD.CIT: Path to a directory where Common Inventory Technology is to be installed
   - TAD.TCD: Path to Tivoli Common Directory
   - TAD.TEMP: Path to a temporary system directory (default: /tmp or %TEMP%)
   - TAD.WINDIR: Path to Windows installation directory
   - TAD.ETC: Path to the etc directory

6. Run the script:
   - TAD.sh
   - TAD.bat

Sample output from the scanner:
Repeat the procedure on other computers where agents are to be installed.

**Extracting .zip installer files on AIX**

If you do not have `unzip` installed on your AIX server, download, install and use the program to be able to extract the Tivoli Asset Discovery for Distributed installers.

**Before you begin**

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

The following Tivoli Asset Discovery for Distributed installers are provided in the `.zip` format on the AIX platform:

- TAD4D-server-7.2.2-aix-ppc64.zip
- ILMT-TAD4D-agent-7.2.2-spb-all.zip
- TAD4D-Unmatched-sw-filter-7.2.2.zip

**Procedure**

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

**Running Common Inventory Technology enabler**

You must run the Common Inventory Technology enabler before installing IBM Tivoli Asset Discovery for Distributed agents on any hosts with guest operating
systems that run either under Microsoft Virtual Server or a VMware server that does not use the VMware Virtual Center. Otherwise, no partition information is available when you install the agents, and they are registered on the administration server with a status of incomplete.

**Before you begin**

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

This task has the following prerequisites:

- All guest operating systems must be active when the script runs.
- Supported versions of VMware Server are ESX 3.0, 3.5, 4.0, and 4.1.
- On Microsoft Virtual Server systems, the Microsoft Virtual Machine Additions service must be installed and active.
- VMware servers, VMware Tools must be installed on the guest operating system.
- **Linux** The enabler requires the compat-libstdc++ library to be installed.
- **Red Hat** The enabler requires the compatibility packs documented in Supported platforms for agents.

The enabler is a script that allows Common Inventory Technology to obtain information about the VMware or Microsoft Virtual Server virtualization environment. You need to run the enabler script on the target host system first, before installing the Tivoli Asset Discovery for Distributed agent, and again after every reboot or VM configuration change.

From version 2.6, Fix Pack 2, the Common Inventory Tool enabler has been enhanced with a detailed report from its execution and some additional features:

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

**Tip:** Use a scheduling service to set up the enabler to run automatically. The script does not provide its own scheduling mechanism, so you need to use an operating system function such as the cron service on UNIX computers. It is advisable to set the scheduling mechanism to run the script every day, but a different frequency might be set depending on the unique configuration of your VMs.

**Note:** The procedure described below installs Common Inventory Technology in the default location. To change it, for example if there is not enough space in the default directory, edit the `CITInstallPath` parameter in the agent installation response file.

**Procedure**

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

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

<table>
<thead>
<tr>
<th>Partitioning technology</th>
<th>Required files</th>
</tr>
</thead>
<tbody>
<tr>
<td>VMware host</td>
<td>Windows wenvmw.exe cpuid.exe retrieve.pl</td>
</tr>
<tr>
<td></td>
<td>Linux wenvmw.sh cpuid dispatcher retrieve.pl</td>
</tr>
<tr>
<td>Microsoft Virtual Server host</td>
<td>Windows wenmsvs.exe cpuid.exe</td>
</tr>
</tbody>
</table>

2. Run the enabler script using the -v option.
   - On a VMware host, run `wenvmw.exe -v`.
   - On a VMware host, run `wenvmw.sh -v`.
   - On a Microsoft Virtual Server host, run `wenmsvs.exe -v`.

Log files `retr.out.txt` and `en_out.txt` are created in the same directory as the directory where you copied the files for the script.

3. Check the logs to see whether the script was run successfully.

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

**Disabling SELinux when installing the agent on RedHat Linux**

Unlike with server installation, the permissive SELinux setting is still too restrictive for agent installation. For some kernel releases, setting SELinux to permissive will prevent the agent from being installed. To avoid this, change the setting to disabled mode.

**Procedure**

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

**Setting up a proxy server**

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

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

- You need to have an IBM HTTP Server installed and running on a dedicated server computer. For details on how to install IBM HTTP Server refer to WebSphere Application Server information center.

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

To define a proxy server for communications between agents and the Tivoli Asset Discovery for Distributed server, complete the following steps:

Procedure

1. Stop the IBM HTTP Server by issuing the following command (or option in the Start menu):
   - AIX /usr/IBMIHS/bin/ apachectl stop
   - UNIX /opt/IBMIHS/bin/ apachectl stop
   - Windows From the Start menu, select IBM HTTP server and then Stop HTTP Server.

2. On the HTTP server edit the httpd.conf file. Find the following section and uncomment the lines in bold:

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

3. In the section LoadModule, add the following lines:
<IfModule mod_proxy.c>
ProxyRequests Off
ProxyPass / http://tad4d_server_IP_address:port/
ProxyPassReverse / http://tad4d_server_IP_address:port/
</IfModule>

4. Open the httpd.conf file, search for the line Listen 80 and change it to Listen 9988. 9988 is the default port used for agent to server communication. Use the appropriate value if you are not using the default one.

5. Start the server by issuing the following command (or option in the Start menu):
   - AIX: /usr/IBMHS/bin/ apachectl start
   - UNIX: /opt/IBMHS/bin/ apachectl start
   - Windows: From the Start menu, select IBM HTTP server and then Start HTTP Server.

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

Performing agent security-related tasks

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

Before you begin

Important: If you defined medium or maximum security level while installing the administration server, ensure that you have enabled a valid certificate for the server and agents. For more information see "Agent preinstallation steps" on page 94.
The following diagram shows 2 tasks:

- creating agent certificates, and
- creating administration server certificates

1. Extract server certificate (REQUIRED in case of medium or maximum level of communication)

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

   **Note:** The server certificate file must be named cert.arm. If a different name is used, the response file or shell installer will accept it but a GSKit error will be reported.

2. Prepare agent certificates for client authentication (REQUIRED in case of maximum level of communication)

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

3. Specify security parameters in response files or agent installation software package blocks, or configure UNIX shell installer before installing agents (REQUIRED)

   The following parameters must be specified before the installation of agents:
   - SecurityLevel
   - ServerCustomSSLCertificate (maximum security only)
   - InstallServerCertificate
   - ServerCertFilePath
   - AgentCertFilePath

   After you have completed these tasks, you can proceed to installing agents using one (or more) of the available methods (tools):
   - Tivoli Configuration Manager
   - native installers
   - Windows Logon Scripts
   - shell installers (UNIX platforms only)

### Installing agents using native installers

Installation scripts or wizards are available for all supported platforms.

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

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

### Installing agents on AIX using native installers

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

- Ensure that the computers on which you plan to install agents meet all necessary requirements. See: Agent hardware and software requirements.
- You must have root privileges.
- If you are installing agents on an AIX host that is partitioned using workload partitions (WPARs) with a logical partition (LPAR), you must install an agent in the LPAR before installing agents in a WPAR.
- You need to ensure that agent is installed on WPAR host (in most cases this is an LPAR).

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

If you decide not to use the response file, you will need to update some parameters in the tlmagent.ini configuration file after the installation. The tlmagent.ini file is located in the /etc directory.

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

If you install Common Inventory Technology in a workload partition in default location (/opt), you will have all the binaries shared with global AIX instance (LPAR) and also available to other workload partitions because by default /opt directory is shared. Configuration files and Common Inventory Technology cache data are not shared between WPARs and the LPAR, and are always separate.

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

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

Procedure

1. Log on to the computer where you want to install the agent as a user with administrative rights.
2. Copy the compressed agent installation package ILMT-TAD4D-agent-7.2.2-native-all.tar.gz (Passport Advantage) or CZT51ML.tar.gz (DVD) to a temporary directory on the agent computer - either from a DVD or from a directory where you store the files downloaded from Passport Advantage. The package contains agent native installers for all supported platforms. This is needed because the operating system generates the .toc file before starting the installation of the fileset.
3. Open the system command line and navigate to the directory where you store the file.
4. Extract the files by running the following command:
gzip -d INSTALLER_COMPRESSED_FILE_NAME.tar.gz

And extract the installer files by issuing the following command:
tar xf INSTALLER_TARBALL_FILE_NAME.tar

In the directory you should have two files:
• ILMT-TAD4D-agent-7.2.2-aix-ppc
• response_file.txt

5. Optional: update the parameters in the response_file.txt file. You need to edit this template response file if one or more parameters should be changed, for example the IP address of the administration server. Perform the following steps:
   a. Edit the response file to customize its parameters to your situation.
   b. Either move the response file to your /etc directory, or set the LMT_RESPONSE_FILE_PATH environment variable to point to the location where the response file is stored. For example: LMT_RESPONSE_FILE_PATH=/tmp/my_response_file.txt. If no environment variable has been set, the installer automatically checks the /etc directory for the response file. If the file cannot be located, the agent is installed with the default parameters.

6. To install the agent, issue the following command:
installp -acgXd ILMT-TAD4D-agent-7.2.2-aix-ppc ILMT-TAD4D-agent

You need to run the command from the directory where you have extracted the installer.

In WPAR environments, issue one of the following commands:
• in WPAR
  installp -acgX -Or ILMT-TAD4D-agent

  Before you launch the above command, you need to ensure that agent is installed on the WPAR host (in most cases this is an LPAR).
• in LPAR:
  syncwpar WPAR_name

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

**Fix Pack 2** To install the agent in a directory different from the default one, choose the installation procedure that is suitable for your version of AIX and the version of Tivoli Asset Discovery for Distributed interim fix that you are using:

<table>
<thead>
<tr>
<th>Interim fix 8 and lower</th>
<th>AIX 5.3 and lower</th>
<th>Use the ILMT_INSTALL_PATH environment variable</th>
<th>AIX 5.3.0.61 and higher</th>
<th>Use User Specified Installation Location (USIL)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interim fix 9 and higher</td>
<td>Installation in custom location is not available</td>
<td>Use User Specified Installation Location (USIL)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- For installations that support the use of the ILMT_INSTALL_PATH environment variable, set the variable to point to your custom location:
  ```bash
  export ILMT_INSTALL_PATH=PATH_TO_DESIRED_LOCATION
  ```
- For installations that support the use of the relocation mechanism that is based on the User Specified Installation Location (USIL), perform the following steps:
a. Create the `custom_location` directory:
   
   ```bash
   mkdir -p /custom_location
   ```

b. Make the directory your User Specified Installation Location (USIL):
   
   ```bash
   mkusil -R /custom_location
   ```

c. Install the agent in this location:
   
   ```bash
   installp -R /custom_location
   installp full_path_to_the_installation_package_dir ILMT-TAD4D-agent-7.2.2-aix-ppc
   ILMT-TAD4D-agent
   ```

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

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

b. Edit the server location parameter in the `tlmagent.ini` file:

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

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

c. Start the agent using the `/usr/bin/startsrc -s tlmagent` command.

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

Verify that the installation was successful - check if the agent appears as active in 
the Web interface. If the agent does not appear in the UI after several minutes, 
check the installation trace logs for information about possible errors.

## Installing agents on IBM i using native installers

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

### Before you begin

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

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

The default agent installation directory is `/var/itlm`. It is not possible to change 
the default installation path.

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

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

2. Copy the SAVF file into a library on the target IBM i computer.
   Example:
   a. Enter the 
      CRTSAVF file_name
   command, to create a save file.
   b. Find this file using an FTP client. By default it should be in the QGPL library.
   c. Replace it with the proper Tivoli Asset Discovery for Distributed agent installer file.

   If you want to install the agent using the response file, you also need to copy the os400_agent.txt file.

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

4. Log in to the node as user with authority to use the RSTLICPGM command.

5. Enter the CRTSAVF file_name command, to create a file.

6. Find this file using an FTP client. It should be in the default lib directory.

7. Replace it with the proper Tivoli Asset Discovery for Distributed agent installer file.

8. To install the agent, enter the following command:

\[
\text{RSTLICPGM LICPGM}(1IBMTLM) \text{ DEV}(*\text{SAVF}) \text{ RLS(V7R2M2) SAVF(LIBRARY\_WHERE\_THE\_SAVF\_FILE\_IS\_PLACED/NAME\_OF\_THE\_SAVF)}
\]

The installer automatically checks the /tmp/itlm directory for the response file. If the file cannot be located, the agent is installed with the default parameters.

9. To verify that the agent has been correctly installed, open the Installed License Programs panel on the IBM i node, and check if there is an entry for 1IBMTLM.

10. If you installed the agent without a response file, specify the server address LMT_SERVER_NAME in the /QIBM/UserData/QITLM/conf/itmagent.ini file and start the agent using the strtcpsvr server(*itmagent) command.

11. To verify that the agent has started, check if it appears as active in the Web interface. If the agent does not appear in the UI after several minutes, check the installation trace logs for information about possible errors.

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

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

Installing agents on HP-UX using native installers

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

108
Before you begin

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

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

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

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

Procedure

1. Log on to the computer where you want to install the agent as a user with administrative rights.
2. Copy the compressed agent installation package ILMT-TAD4D-agent-7.2.2-native-all.tar.gz (Passport Advantage) or CZT51ML.tar.gz (DVD) to a temporary directory on the agent computer - either from a DVD or from a directory where you store the files downloaded from Passport Advantage. The package contains agent native installers for all supported platforms.
3. Open the system command line and navigate to the directory where you store the compressed package.
4. Extract the files by running the following command:
   
   gzip -d INSTALLER_COMPRESSED_FILE_NAME.tar.gz

   And extract the installer files by issuing the following command:

   tar xf INSTALLER_TARBALL_FILE_NAME.tar

   In the directory you should have two files:
   - ILMT-TAD4D-agent-7.2.2-hpux
   - response_file.txt

5. response_file.txt is a template response file. If you want to install the agent with the response file, update the parameters in the file. See UNIX(r) agents installation response file for more information. You will be able to reuse the response file in any other agent installations on systems with the same configuration. To do so, copy it to the /etc directory on any machine where you want to reuse it.

6. To install the agent enter the following command:

   swinstall -s ABSOLUTE_PATH_TO_INSTALLER_FILE/ILMT-TAD4D-agent-7.2.2-hpux ILMT-TAD4D-agent:/INSTALL_PATH

   swinstall -s ABSOLUTE_PATH_TO_INSTALLER_FILE/ILMT-TAD4D-agent-7.2.2-hpux -x enforce_dependencies=false

   ILMT-TAD4D-agent:/INSTALL_PATH

   The installer automatically checks the /etc directory for the response file. If the file cannot be located, the agent is installed with the default parameters.

7. To verify that the installation has been successful, check if the agent appears as active in the Web interface. If the agent does not appear in the UI after several minutes, check the installation trace logs for information about possible errors. If the installation fails, the registry entry will state that the agent is installed properly. You need to run the agent uninstallation command.
If you installed the agent without the response file, it is configured to connect to a server located on the local host. If your server is installed on a different computer, use the tlmagent -e command to stop the agent, edit the server location parameter in the tlmagent.ini file:

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

then start the agent using the tlmagent -g command.

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

### Installing agents on Linux using native installers

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

#### Before you begin

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

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

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

#### Procedure

1. Log on to the computer where you want to install the agent as a user with administrative rights.

2. Copy the compressed agent installation package `ILMT-TAD4D-agent-7.2.2-native-all.tar.gz` (Passport Advantage) or `CZT51ML.tar.gz` (DVD) to a temporary directory on the agent computer - either from a DVD or from a directory where you store the files downloaded from Passport Advantage. The package contains agent native installers for all supported platforms.

3. Open a system command prompt and navigate to the directory where you store the file.

4. Extract the installer files using the following command:

   ```
tar xzvf INSTALLER_COMPRESSED_FILE_NAME.tar.gz
   
   In the directory you should have two files:
   ```
   ```
   • `ILMT-TAD4D-agent-7.2.2-linux-x86.rpm` (Linux x86), or
   • `ILMT-TAD4D-agent-7.2.2-linux-ppc.rpm` (Linux ppc), and
   • `response_file.txt`
   
   5. `response_file.txt` is a template response file. If you want to install the agent with the response file, update the parameters in the file. See *UNIX(r) agents installation response file* for more information.

   - Set the `LMT_RESPONSE_FILE_PATH` environment variable to point to the location of the response file.

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

6. Enter the following command:

   `rpm -Uvh ILMT-TAD4D-agent-7.2.2-linux-x86.rpm`

   or

   `rpm -Uvh ILMT-TAD4D-agent-7.2.2-linux-ppc.rpm`

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

   `rpm -Uvh ILMT-TAD4D-agent-7.2.2-linux-x86.rpm --prefix full_installation_path`

   If no environment variable has been set, the installer automatically checks the `/etc` directory for the response file. If the file cannot be located, the agent is installed with the default parameters.

7. To verify that the installation has been successful, check if the agent appears as active in the Web interface. If the agent does not appear in the UI after several minutes, check the installation trace logs for information about possible errors. If the installation fails, the registry entry will state that the agent is installed. You need to run the agent uninstallation command.

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

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

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

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

**Installing agents on Linux on System z**

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

**Before you begin**

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

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

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

**Procedure**

1. Log on to the computer where you want to install the agent as a user with administrative rights.

2. Copy the compressed agent installation package `ILMT-TAD4D-agent-7.2.2-native-all.tar.gz` (Passport Advantage) or `CZT51ML.tar.gz` (DVD) to a temporary directory on the agent computer - either from a DVD or from a
directory where you store the files downloaded from Passport Advantage. The package contains agent native installers for all supported platforms.

3. Open the system command line and navigate to the directory where you store the file.

4. Uncompress the file and extract the installer files using the following command:
   
   ```
   tar xzvf INSTALLER_COMPRESSED_FILE_NAME.tar.gz
   ```
   
   In the directory you should have two files:
   
   - ILMT-TAD4D-agent-7.2.2-linux-s390.rpm (for Linux on System z), and
   - response_file.txt

5. To install the agent, you need to update the parameters in the response file and copy it to the etc directory. response_file.txt is a template response file. See UNIX(r) agents installation response file for more information.

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

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

   **MachineType**
   This is a new parameter introduced in Tivoli Asset Discovery for Distributed 7.2.1. The possible values are z9® or z10™ (Specify z10 if you are installing the agent on a server computer with the z196 processor).

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

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

   **SystemActiveProcessors**
   This is the total number of all active processors (CP and IFL) in a physical machine.

   **MessageHandlerAddress**
   Specify the hostname or IP address of the Tivoli Asset Discovery for Distributed server. Message handler is a server component which manages incoming and outgoing agent data.

   **Note:** If you do not set the MessageHandlerAddress parameter, the agent is configured to connect to a server located on the local host. If your server is installed on a different machine, use the tlmagent -e command to stop the agent, and edit the server location parameter in the tlmagent.ini file located in the /etc directory:

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

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

   If no values are specified, the installation will fail.
7. Enter the following command:
   \texttt{rpm -Uvh ILMT-TAD4D-agent-7.2.2-linux-s390.rpm}
   
   To install the agent in a directory different from the default one, enter:
   \texttt{rpm -Uvh ILMT-TAD4D-agent-7.2.2-linux-s390.rpm --prefix full_installation_path}
   
   If no environment variable has been set, the installer automatically checks the /etc directory for the response file. If the file cannot be located, the agent is installed with the default parameters.

8. To verify that the installation has been successful, check if the agent appears as active in the Web interface. If the agent does not appear in the UI after several minutes, check the installation trace logs for information about possible errors. If the installation fails, the registry entry will state that the agent is installed. You need to run the agent uninstallation command.

**Installing agents on Solaris using native installers**

You can install agents on Solaris platforms using the \texttt{pkgadd} command.

**Installing agents interactively**

If you decide to use this method, you will need to make choices and respond to command line prompts when installing the agents.

**Before you begin**

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

The default agent installation directory is /var/itm. To install the agent in a different directory, specify the \texttt{AgentInstallPath} parameter in the response file.

**Important:** If you are installing agents on a Solaris platform that is partitioned using the Containers partitioning technology, the HostID of the local zone must be the same as the HostID of the global zone.

**Note:**

1. If you are installing agents on a Solaris 10 platform that is partitioned using the Containers partitioning technology, you must first install the agent in the global zone. The agent will automatically be installed also in all existing and future local zones. On a Solaris 11 platform, you must install the agent in the global zone and in every local zone separately.

2. If a Solaris platform is partitioned using the Containers partitioning technology, and you want to install an agent using the response file, you need to copy the response_file.txt files to the /etc directory on each zone (global and local).

3. Make sure that the status of agents on both zones is the same. If you are installing the agent for the first time, ensure that there are no agents already installed on either global or local zones.

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

5. Make sure that the console width is set to a maximum of 168 columns.

**Procedure**

1. Log on to the computer where you want to install the agent as a user with administrative rights.
2. Copy the compressed agent installation package ILMT-TAD4D-agent-7.2.2-native-all.tar.gz (Passport Advantage) or CZT51ML.tar.gz (DVD) to a temporary directory on the agent computer - either from a DVD or from a directory where you store the files downloaded from Passport Advantage. The package contains agent native installers for all supported platforms.

3. Open a system command prompt and navigate to the directory where you store the file.

4. Extract the installer files by running the following command:
   
   ```
gzip -d installer_compressed_file_name.tar.gz
   ```
   And extract the installer files by issuing the following command:
   ```
tar -xf installer_tarball_file_name.tar
   ```
   In the directory, there should be four files:
   - ILMT-TAD4D-agent-7.2.2-solaris-x86_64 (Solaris on EM64T and AMD 64), or
   - ILMT-TAD4D-agent-7.2.2-solaris-sparc32 (Solaris on SPARC, 32-bit), or
   - ILMT-TAD4D-agent-7.2.2-solaris-sparc64 (Solaris on SPARC, 64-bit), and
   - response_file.txt, and
   - update_contents.sh, and
   - installer_tarball_file_name.tar

5. response_file.txt is a template response file. If you want to install the agent with the response file, update the parameters in the file and copy it to the /etc directory. See “UNIX agents installation response file” on page 131 for more information.

6. Install the agent by running the command:
   ```
pkgadd -d ILMT-TAD4D-agent-7.2.2-platform ILMT-TAD4D-agent
   ```
   **Important:** If you are installing agents on a Solaris 11 platform that is partitioned using the Containers partitioning technology, you must run the installation command on every zone separately.

7. To verify that the installation has been successful, check if the agent appears as active in the Web interface. If the agent does not appear in the user interface after several minutes, check the installation trace logs for information about possible errors. If the installation fails, the registry entries will state that the agent is properly installed. You need to run the agent unistallation command.
   - If you installed the agent without the response file, it is configured to connect to a server located on the local host. If your server is installed on a different computer, use the tlmagent -e command to stop the agent, and edit the server location parameter in the tlmagent.ini file:
     ```
     # Preferred Server
     # (Reloadable: No)
     server = IP_ADDRESS
     ```
     Then, start the agent using the tlmagent -g command.

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

   **Important:** If you want to enable self-update for an agent installed on bare metal Solaris 10, you must restart the agent after installation.
Installing agents on Windows using a native installer

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

Before you begin

Ensure that the computers on which you plan to install agents meet all necessary requirements. See: Planning the installation of agents.

The default agent installation directory is %WINDIR%\itlm. If you want to install the agent in a different directory, specify the Agent destination folder parameter as described in step 8.

Note:
1. The IBM Tivoli Asset Discovery for Distributed installer does not support file names with double-byte characters including log file names and response file names.
2. The agent installer does not check for the disk space available for the Common Inventory Technology installation.

Installing agents interactively

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

Procedure

1. Log on to the computer where you want to install the agent as a user with administrative rights.
2. Copy the compressed agent installation package CI27RML.tar.gz to a temporary directory on the agent computer - either from a DVD or from a directory where you store the files downloaded from Passport Advantage. The package contains agent native installers for all supported platforms.
3. Extract the installer files using a utility that supports the tar, and gz formats. The main file setup.exe is located in directory temp_dir\ILMT-TAD4D-agent--windows-x86.
4. Click setup.exe to launch the installation wizard.
5. Select the language version that you want to install and click Next.
6. A welcome panel opens. Click Next.
7. Select the installation type:
   - Custom
     Allows you to specify all parameters.
   - Typical
     Allows you to specify only the server address. It also enables you to save your settings in a response file. You can browse your file system and determine the directory where the response file is to be saved. All other agent parameters are set to default values.
     In this scenario, Custom is selected, showing the parameters that are available and their default settings. Click Next.
8. Specify the agent parameters:
Agent destination folder
The folder in which the agent files are installed. You can override the default installation path for the agent by changing the path shown here.

Note: It is impossible to install agents in 64-bit Windows directory Program Files. If you install the agent in c:\Program Files on 64-bit Windows, this path will be changed to the 32-bit directory c:\program files(x86).

Agent temporary folder
The folder in which the agent installer stores files during the installation process

Common Inventory Technology destination folder
The folder in which the Common Inventory Technology files will be installed.

Click Next.

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

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

HTTP To use nonsecure communication (minimal security).

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

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

Note:
a. Agents with minimum and medium security levels can communicate with a server that has security levels of minimum or medium provided that both the secure and nonsecure ports are configured. If the maximum security level is used, both the agent and the server must be aligned with the security level set to maximum.

b. If you select medium or maximum security, you must set up and install the certificates. For full information about enabling security, see the "Security" section of the Tivoli Asset Discovery for Distributed information center.

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

Install certificate
Selecting this option activates the Server certificate file group box in the lower part of the panel and enables the installation of the security certificate (not applicable if you choose minimum security option).

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

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

In the Agent certificate file group box, specify the following:

Install agent certificate file
Selecting the Install agent certificate file check box allows you to specify the path to the certificate file below.

Click Next.

10. On the Connection parameters panel specify the following agent parameters:

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

Port
This enables you to specify the port number that the agent uses to communicate with the server. The default is 9988. If there is a star in front of the port name, the corresponding security level has been selected on the previous pane.

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

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

Under Proxy Settings, specify the following:

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

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

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

11. On the Advanced configuration panel specify the following parameters:
Scan group
The name of the scan group that the agent belongs to.

Click Next.

12. A summary panel opens. Select the check box **Install the agent**. If you plan to install the agent on computers with the same configuration, select the check box **Save my settings in a response file** and click **Browse** to specify the folder where the file is to be saved. Click **Next** to start the installation of the agent.

13. When the installation is complete, click **Finish**.

**Installing agents silently**

**Procedure**

1. Log on to the computer where you want to install the agent as a user with administrative rights.

2. Copy the CI27RML.tar.gz file to a directory in the file system of your computer (either from a DVD or a directory where you store the files downloaded from Passport Advantage). Extract the compressed file into a directory on your disk.

3. Start the command-line interface and change to the directory where you have extracted the files.

4. Type: `setup.exe /z"/s"%drive_letter%\path_to_response_file_dir\response_file.txt" /L%language% /s`. This command uses the following parameters:

   - **response_file**
     The full path to the agent response file.

   - **language**
     The code of the language that you want to use for the upgrade. The following language codes are available:

     | Code   | Language                        |
     |--------|---------------------------------|
     | 1033   | English (United States)         |
     | 1036   | French (France)                 |
     | 1041   | Japanese                        |
     | 1042   | Korean                          |
     | 1029   | Czech                           |
     | 1060   | Slovenian (Slovenia)            |
     | 2052   | Chinese (PRC)                   |
     | 1031   | German (Germany)                |
     | 1034   | Spanish (Traditional Sort)      |
     | 1045   | Polish                          |
     | 1049   | Russian                         |
     | 1038   | Hungarian                       |
     | 1043   | Dutch (Netherlands)             |
     | 1050   | Croatian                        |

   Example:
   `setup.exe /z"/s"%sfc%\Temp\response_file.txt" /L1033 /s`

   **Note:** To install the agent in a custom directory, specify the directory name as the value of the environment variable:
   `ILMT_INSTALL_PATH=agent_install_directory`

You have installed version agent in silent mode.

**Rerunning a failed agent installation**

Agent installation consists of three phases: preinstallation, installation (copying of files) and postinstallation during which agent configuration takes place. Installation might fail during the first or third phase. The way to reinstall an agent depends on the phase during which the error occurred.
Rerunning agent installation that failed in the preinstallation phase
If the agent installation failed in the preinstallation phase, you can rerun the native installer after you have diagnosed and remedied the error.

Procedure
1. Find the cause of the problem by examining the file:
   - **UNIX**: `/tivoli_common_directory/logs/install/trace/ILMT-TAD4D-agent-pre-date_of_the_event-hourminute.trc`
   - **Windows**: `\tivoli_common_directory\logs\install\trace\ILMT-TAD4D-agent-pre-date_of_the_event-hourminute.trc`
2. Correct the problem. The reason of failure might be, for example, lack of sufficient write rights.
3. Retype the agent installation command.

Rerunning agent installation that failed in the postinstallation phase
If the agent installation failed in the postinstallation phase, you have two possibilities to finalize it: you can rerun the configuration process or force the installation.

Procedure
1. Find the cause of the problem by examining the file
   - **UNIX**: `/tivoli_common_directory/logs/install/trace/traceDeployagent.log`
   - **Windows**: `\tivoli_common_directory\logs\install\trace\traceDeployagent.log`
2. Correct the problem.
3. Finalize the installation.
   - Force the installation of the agent by issuing the following command:
     - **AIX**: `installp -acFXd ILMT-TAD4D-agent-7.2.2-aix-ppc ILMT-TAD4D-agent`
     - **HP-UX**: `swinstall -s reinstall=true ABSOLUTE_PATH_TO_INSTALLER_FILE/ILMT-TAD4D-agent-7.2.2-hpux ILMT-TAD4D-agent:<INSTALL_PATH>`
     - **IBM i**: `RSTLCPGM LICPGM(1IBMTLM) DEV(*SAVF) RLS(V7R2M2) SAVF(LIBRARY.Where.The.SAVF.File.Is.Placed/NAME_Of_The.SAVF)`
     - **Linux**: `rpm -Uvh --force ILMT-TAD4D-agent-7.2.2-linux-platform.rpm`
     - **Solaris**: `pkgadd -d ILMT-TAD4D-agent-7.2.2-solaris-platform ILMT-TAD4D-agent`
   Open the `/var/sadm/install/admin/default configuration file, and change instance=line to instance=overwrite or instance=ask. Otherwise, the package will not be installed.
   - **Windows**: Run the interactive installer, specifying all necessary parameters.
Installing agents on UNIX using shell installers

Install your agents on UNIX platforms using shell installers. It is not necessary to edit and copy the response file to the target directory. All the parameters that you supply are validated on the run.

Before you begin

Create a User Specified Installation Location (USIL) if you want to install the agents in a non-standard location.

The Tivoli Asset Discovery for Distributed agent shell installation packages are available on the Passport Advantage website (and on the product DVD).

There are two types of shell installers:

- Separate installer files for individual UNIX platforms.
  - AIX: ILMT-TAD4D-agent-7.2.2-aix-ppc.bin
  - HP-UX: ILMT-TAD4D-agent-7.2.2-hpux.bin
  - Linux:
    - ILMT-TAD4D-agent-7.2.2-linux-x86.bin
    - ILMT-TAD4D-agent-7.2.2-linux-s390.bin
    - ILMT-TAD4D-agent-7.2.2-linux-ppc.bin
  - Solaris:
    - ILMT-TAD4D-agent-7.2.2-solaris-sparc32.bin
    - ILMT-TAD4D-agent-7.2.2-solaris-sparc64.bin
    - ILMT-TAD4D-agent-7.2.2-solaris-x86_64.bin
  - UNIX: ILMT-TAD4D-agent-7.2.2-multi_unix.bin

You can get these files by uncompressing the file ILMT-TAD4D-agent-7.2.2-shell-all.tar.gz. Use a separate-platform shell installer if you want to install numerous agents with the same parameters on one platform.

- One installer that can be used on all UNIX platforms: ILMT-TAD4D-agent-7.2.2-multi_unix.bin. Use this shell installer if you want to install many agents with the same parameters on different platforms.

Procedure

1. Open the command-line interface and navigate to the directory where you store the shell installer.
2. (optional) Run the following command to obtain all the installation parameters:
   - `./installer_file_name.bin -get` to obtain platform-specific parameters (both types of installer),
   - `./installer_file_name.bin -get_all` to obtain parameters for all supported platforms (ILMT-TAD4D-agent-7.2.2-multi_unix.bin only).

You might also want to use other installation options:

- **-help** Returns the information about available installation options.
- **-extract**
  Extracts the native installer and its response file to a temporary directory.
3. Run the following command to set the installation parameters:
   - `./installer_file_name.bin -set` to set platform-specific parameters (both types of installer),
When installing the agent on AIX, specify if you want to install the agent in a shared WPAR. To do that:

a. Run the installation script: "./ILMT-TAD4D-agent-7.2.2-aix-ppc.bin -set"

b. Supply all necessary parameters.

c. Set `InstallOnWpars` to `y`.

You can install the agent in a directory different from the default one on AIX version 5.4 and higher by using the relocation mechanism that is based on the `User Specified Installation Location` (USIL). To install the agent in a custom location:

a. Create the `custom_location` directory:
   
   `mkdir -p /custom_location`

b. Run the installation script: "./ILMT-TAD4D-agent-7.2.2-aix-ppc.bin -set"

c. Set the `AixCustomLocation` parameter to point to your custom location.

When installing the agent on Solaris, specify if you want to install the agent in a local zone. To do that:

a. Run the script: "./ILMT-TAD4D-agent-7.2.2-solaris-sparc64.bin -set"

b. Supply all necessary parameters.

c. Set `InstallOnZones` to `y`.

Enter the following command if you want to write default parameters to the shell installer:

```
./installer_file_name.bin -restore_defaults
```

4. Run the following command to install the agents: "./installer_file_name.bin -install"

**Note:** Ensure that the agent certificate file is readable for any user and is located in a directory path that has read permissions set for all users. Typically, a user "nobody" or "install" is used for doing preinstallation checks. If a certificate file is owned by superuser and not available for reading to an installation user, the installation will fail. If you do not set proper read permissions, you will not be able to install the agent with the maximum security level.

You have installed the agent on a given UNIX platform.

If you have installed an agent on a logical partition (LPAR) on an AIX 5.2 host that is partitioned using workload partitions (WPars), you must perform additional configuration steps to make sure that the server capacity is reported correctly. For more information on how to do that, see [Configuring the node core capacity](#).

---

**Using IBM Tivoli Configuration Manager to install the agents in bulk**

For environments where IBM Tivoli Configuration Manager is installed, you can use its software distribution function to deploy the agents to endpoints as software packages.
Before you begin

Ensure that you have the appropriate version of Tivoli Configuration Manager and Tivoli Management Framework installed in your environment:

**IBM Power Systems platforms**
- Management Framework 4.1 with fixes 4.1-TMF-0015 for Linux-PPC (server) and 4.1-INVGW-0005 for Linux-PPC (gateway) installed
- Configuration Manager 4.2 with fixes 4.2-SWD-0014 (server) and 4.2-SWD-0015 (gateway) installed

**IBM System z platforms**
- Management Framework 4.1.1
- Configuration Manager 4.2.1

**Other platforms**
- Management Framework 4.1
- Configuration Manager 4.2.

Depending on the platform, you also need 20 – 30 MB of disk space for the software package block that is to be distributed.

**AIX** Create a *User Specified Installation Location* (USIL) if you want to install the agents in a non-standard location on AIX

The Tivoli Asset Discovery for Distributed Software Package DVD contains an agent installation SPB for each supported platform:
- **AIX** agent_aix_ppc.spb
- **HP-UX** agent_hpux.spb
- **IBM i** agent_os400.spb
- **Linux** agent_linux_x86.spb
- **Linux** agent_linux_s390.spb
- **Linux** agent_linux_ppc.spb
- **Solaris** agent_solaris_32.spb
- **Solaris** agent_solaris_64.spb
- **Solaris** agent_solaris_x86.spb
- **Windows** agent_win32.spb

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

**Procedure**
1. Copy the software package block for your platform from the DVD to a directory on the TMR server or a managed node.
2. Ensure that the Tivoli Environment is configured.
3. Create a profile manager for each SPB that you want to distribute.
4. Import the SPBs.
5. Perform distributions using the force option to install the appropriate platform-specific agent SPB on each target computer.

You must provide values for the configuration parameters during the distribution. See the related links section for a complete definition of the software package block and the possible values that can be assigned to each parameter. When installing agents on Linux on System z provide the values for the following parameters: MachineType, ProcessorType, SharedPoolCapacity, SystemActiveProcessors, and MessageHandlerAddress.

**Note:** When updating agents installed in a non-default directory, the value of the `agt_custom_location` parameter value has to be set to that directory. For example, `agt_custom_location=/opt/itlm` for the agent is installed in the `/opt/itlm` directory.

If you have installed an agent on a logical partition (LPAR) on an AIX 5.2 host that is partitioned using workload partitions (WPARs), you must perform additional configuration steps to make sure that the server capacity is reported correctly. For more information on how to do that, see [Configuring the node core capacity](#).

### Software package parameters

The tables list the parameters for deploying IBM Tivoli Asset Discovery for Distributed agents using Tivoli Configuration Manager.

#### Common parameters

**Table 27. Common parameters**

<table>
<thead>
<tr>
<th>Parameter name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AgentCertFilePath</td>
<td>If you have selected to supply certificates (InstallServerCertificate) and you are using security level 2, you need to specify the path to the CMS keystore which contains the agent certificate, specific to the agent that is to be deployed. The password of this keystore must be set to <code>slmtest</code>. The default value of this parameter is <code>none</code>.</td>
</tr>
<tr>
<td>AgentTempPath</td>
<td>To override the location where agent keeps the working files, enter a valid path.</td>
</tr>
<tr>
<td>CITInstallPath</td>
<td>Specify the Common Inventory Technology installation folder.</td>
</tr>
<tr>
<td>FipsEnabled</td>
<td>Set to <code>y</code> to enable encryption of data using a FIPS-approved algorithm. The default is <code>n</code>.</td>
</tr>
<tr>
<td>InstallServerCertificate</td>
<td>If you have selected <code>SecurityLevel=1</code> or <code>SecurityLevel=2</code>, you can choose to install certificates. Possible values are:</td>
</tr>
<tr>
<td></td>
<td><code>y</code> Install the server certificate defined in <code>ServerCertFilePath</code> or agent certificate defined in <code>PrivateKeyCertFilePath</code>, or both. If <code>ServerCertFilePath=none</code>, the server test certificate will be installed.</td>
</tr>
<tr>
<td></td>
<td><code>n</code> Do not install any certificate file.</td>
</tr>
<tr>
<td>MessageHandlerAddress</td>
<td>Specify the hostname or IP address of the Tivoli Asset Discovery for Distributed server. Message handler is a server component which manages incoming and outgoing agent data. This is a mandatory parameter.</td>
</tr>
<tr>
<td>ProxyAddress</td>
<td>If <code>UseProxy</code> is <code>y</code>, enter the address (host name or IP address) of the proxy server.</td>
</tr>
<tr>
<td>ProxyPort</td>
<td>The port number on which the proxy server listens, if applicable. If <code>UseProxy</code> is <code>y</code>, enter the port of the proxy server.</td>
</tr>
<tr>
<td>ScanGroup</td>
<td>The name of a scan group that has been created in the Tivoli Asset Discovery for Distributed server database.</td>
</tr>
</tbody>
</table>
Table 27. Common parameters (continued)

<table>
<thead>
<tr>
<th>Parameter name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SecureAll</td>
<td>The port number used by the agent to communicate with the Tivoli Asset Discovery for Distributed server. This value is used if the level of security has been set to 2. The default is 9977.</td>
</tr>
<tr>
<td>SecureAuth</td>
<td>The port number used by the agent to communicate with the Tivoli Asset Discovery for Distributed server. This value is used if the level of security has been set to 1. The default is 9999.</td>
</tr>
<tr>
<td>SecurityLevel</td>
<td>The level of security to be used for communication between the agent and the Tivoli Asset Discovery for Distributed server. Valid values are: 0 To use nonsecure communication. 1 To use secure communications with server authentication. 2 To use secure communications with client and server authentication. Note: 1. The Tivoli Asset Discovery for Distributed server configured for maximum security can communicate with agents set to maximum security only. If the server is configured to use medium security, then only agents set to medium or maximum security can connect to it. A server configured for minimum can support agents set for any security level. 2. If you select medium or maximum security, you must perform a series of tasks to set up and install certificates. For full information about enabling security, see the “Security” section of the information center.</td>
</tr>
<tr>
<td>ServerCertFilePath</td>
<td>If you have selected to supply certificates (InstallServerCertificate=y), you can choose to provide your own server certificate to be used for server authentication by the agent (SecurityLevel&gt;0). Possible values are: path/cert.arm - Indicates that you want to provide your own server certificate. none - Indicates that you want to use the server test certificate. The name of the server certificate must be cert.arm. If the path contains spaces, enclose the whole path in double-quotes. Note: The test certificate may only be used for test purposes as it is in the name of IBM and is insecure (the same certificate is distributed to all customers). Use the Data Moving Service in Tivoli Configuration Manager to simultaneously copy the cert.arm file to multiple computers.</td>
</tr>
<tr>
<td>ServerCustomSSLCertificate</td>
<td>If you have selected to supply SSL certificate (InstallServerCertificate=y), you can choose to provide your own server certificate to be used by the agent for secure communications with the server. Possible values are: y Indicates that you want to provide your own server certificate. n Indicates that you want to use the server test certificate. Note that the test certificate may only be used for test purposes as it is in the name of IBM and is insecure (the same certificate is distributed to all customers). If you select the value &quot;y&quot;, you must also supply the certificate pathname (ServerCertFilePath). For example, to indicate that you want to use your own server certificate for SSL communication, use the following: ServerCustomSSLCertificate=y</td>
</tr>
<tr>
<td>ServerPort</td>
<td>The port number used by the agent to communicate with the Tivoli Asset Discovery for Distributed server. This value is used if the level of security has been set to 0. The default is 9988.</td>
</tr>
</tbody>
</table>
### Table 27. Common parameters (continued)

<table>
<thead>
<tr>
<th>Parameter name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>UseProxy</td>
<td>Set to y if a proxy port is to be used for communications between agents and the Tivoli Asset Discovery for Distributed server. The default is n.</td>
</tr>
</tbody>
</table>

### Parameters for Linux on System z only

**Table 28. Parameters for Linux on System z**

<table>
<thead>
<tr>
<th>Parameter name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MachineType</td>
<td>Type of the machine (CP or IFL). The default is IFL.</td>
</tr>
<tr>
<td>ProcessorType</td>
<td>Type of the processor (CP or IFL). The default is IFL.</td>
</tr>
<tr>
<td>SharedPoolCapacity</td>
<td>The number of shared processors of a given type (CP or IFL) on the server</td>
</tr>
<tr>
<td>SystemActiveProcessors</td>
<td>The total number of processors in the computer</td>
</tr>
</tbody>
</table>

### Solaris parameter

**Table 29. Solaris parameter**

<table>
<thead>
<tr>
<th>Parameter name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>InstallOnDD</td>
<td>Installation on Dynamic Domain</td>
</tr>
<tr>
<td></td>
<td>Possible values are:</td>
</tr>
<tr>
<td>y</td>
<td>Indicates that the agent is being installed on Dynamic Domain.</td>
</tr>
<tr>
<td>n</td>
<td>Indicates that the agent is not being installed on Dynamic Domain.</td>
</tr>
</tbody>
</table>

### Installation-related parameters (UNIX and Windows platforms)

**Table 30. Installation-related parameters on UNIX and Windows platforms**

<table>
<thead>
<tr>
<th>Parameter name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>agt_logs_dir</td>
<td>The directory where the installer logs are to be written. The default is not to log the installation information.</td>
</tr>
<tr>
<td>agt_custom_location</td>
<td>The name of the directory in which agents are to be installed. The default value is agt_custom_location=/usil.</td>
</tr>
<tr>
<td></td>
<td>This parameter is optional.</td>
</tr>
<tr>
<td>agt_temp_dir</td>
<td>Software Package Blocks use this folder to store temporary files.</td>
</tr>
<tr>
<td>agt_temp_path</td>
<td>The location of temporary agent files on the agent computer. The default value depends on the platform (/ttm subdirectory in the temporary directory). For more information, see the related reference section.</td>
</tr>
<tr>
<td>tcm_logs_dir</td>
<td>The directory where the Tivoli Configuration Manager logs are to be written. The default is $(agt_temp_path).</td>
</tr>
</tbody>
</table>

### Installing agents with Windows logon scripts

As an alternative to using the interactive installation wizard, you can install the IBM Tivoli Asset Discovery for Distributed agents on Windows targets by using the operating system facility that runs a script when users log on to the Windows domain.
The script checks if there is an agent on the computer the user has logged on, and if it detects an agent, whether it is the same version. If the script finds no agent or a back-level agent, it installs the agent.

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

**Procedure**

1. Log on to the Windows domain controller.
2. Find or create the NETLOGON shared directory. You should not grant write permissions to the directory to all users in the domain. The contents of the shared directory should be as follows:
   - `getdt.exe`
   - `gethost.exe`
   - `getos.bat`
   - `printmsg.exe`
   - `profiles`
   - `setAgentReturnCode.bat`
   - `sethostname.bat`
   - `setup.exe`
   - `tlm.bat`
   - `tlminstall.bat`
   - `profiles/default.conf`
   
   You can locate those files in the .zip archive containing the latest version of the Tivoli Asset Discovery for Distributed agent for the Windows platform, for example, `7.2.2-TIV-ILMT-TAD4D-FP00001-agent-windows-x86.zip`.

   If the user account that you are using for the installation has Domain Administrator rights, you can also set up a shared directory for logs so that the actions of the scripts are logged on the domain server.

3. Specify the script `tlm.bat` in the user profile of the Domain User Manager. Set the script to run automatically when logging in to the domain account.

4. Set the following values for the environment variables in the `tlm.bat` file in the NETLOGON directory:

   ```
   set DOMAINSERVER=DOMAIN_SERVER
   set NETLOGON_SHARE=NETLOGON_SHARE
   set LOG-share=LOG_SHARE
   set INSTALL_PATH=INSTALL_PATH
   ```

   where:

   - **DOMAIN_SERVER**
     The host name of the Windows domain controller.

   - **NETLOGON_SHARE**
     The share name of the NETLOGON share.

   - **LOG_SHARE**
     The share name of the LOG share where the logs are to be stored. If you do not want to log the running of the script, change the variable to blank.
INSTALL_PATH
(Optional) The name of the non-default directory where you want to
install the agent. If you want to use the default installation path, do not
provide a value for the INSTALL_PATH variable. If the specified
installation path contains spaces, it must be enclosed in quotes.

5. Set the agent installation parameters in the profiles\default.conf
configuration file. You must configure parameter values for the server. You can
leave the other parameters as defaults.
   • If you are assigning all computers in the domain to the same organization,
     scan group, and server, you can use this file to deploy all the agents.
   • If you are assigning some computers a different configuration, you can create
copies of the default file, named profiles\hostname.conf (where hostname is
the host name of the computer to which the configuration is to be applied)
and define different configurations in these files.

For parameter descriptions, see “Windows agent installation response file and
logon script configuration file” on page 129.

6. Log on to the system on which the agent is to be installed. Use the domain
user account.

   Note: Ensure that you belong to the local Administrators group on the
computer where the agent is installed.

7. If the IBM Global Security Kit (GSKit) is already in use, reboot the computer to
complete the installation.

Performing a refresh installation of agents

If you perform a refresh installation of IBM Tivoli Asset Discovery for Distributed
agents, you can refresh them without changing their configuration parameters. You
can do this by reinstalling them manually.

Before you begin

Solaris If you are using the native installation script, you need to open the
/var/sadm/install/admin/default configuration file, and change instance=line to
instance=overwrite. Otherwise, packages will not be refreshed.

Procedure
1. Copy the compressed installer to a directory in the file system of your
   computer (either from a DVD or a directory where you store the files
downloaded from Passport Advantage).
2. Open the system command line and navigate to the directory where you store
   the compressed installer.
3. Uncompress the file by running the following command:
   gzip -d INSTALLER_TARBALL_FILE_NAME.tar.gz
4. Extract the installer files by issuing the following command:
   tar xf INSTALLER_TARBALL_FILE_NAME.tar

   Depending on your platform, in the directory, there should be the following
   files:
   • AIX
     – ILMT-TAD4D-agent-aix-ppc
     – ILMT_TAD4D_7.2.2_agentInstall_response.txt
5. To perform a refresh installation of an agent enter the following command:

- **AIX**
  
  `installp -acgXd PATH_TO_INSTALLATION_PACKAGE_DIR ILMT-TAD4D-agent`

  In WPAR environments, the command is:
  
  `installp -acgX -Or ILMT-TAD4D-agent`

  If the agent was installed using a native installer the command is:
  
  `installp -acFXd PATH_TO_INSTALLATION_PACKAGE_DIR ILMT-TAD4D-agent`

  In WPAR environments, the command is:
  
  `installp -acFX -Or ILMT-TAD4D-agent`

- **HP-UX**
  
  `swinstall -s INSTALLER_FILE_NAME ILMT-TAD4D-agent`

  If the agent was installed using a native installer the command is:
  
  `swinstall -s INSTALLER_FILE_NAME ILMT-TAD4D-agent`

- **Linux**
  
  `rpm -Uvh INSTALLER_FILE_NAME.rpm`

  If the agent was installed using a native installer the command is:
  
  `rpm -Uvh --force INSTALLER_FILE_NAME.rpm`

- **Solaris**
  
  `pkgadd -d INSTALLER_FILE_NAME`

  If the agent was installed using a native installer, use the same command.

The agent files on your computer have been refreshed.

---

**Image cloning with preinstalled agents**

Use the VM cloning feature to create a golden image with an agent that was already installed.
You can run the `tlmagent -clone` command to configure the agent to work properly after it is cloned. Then, you can clone the image and new agents will plug in to the server.

To configure the agents to work after VM images are cloned, complete the following steps:

**Procedure**

1. Install the agent.
2. Provide the Tivoli Asset Discovery for Distributed server address in the `tlmagent.ini` file.
3. Run the following command: `tlmagent -clone`
4. Clone the golden image.
5. Log on to the system that was cloned and start the agent.

**Note:** If you install the agent on the golden image and plug it into the server before you run the `tlmagent -clone` command, this agent is registered on the server and displayed in the Agent window. You can remove this agent from the server.

---

**Agent installation response files**

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

**Windows agent installation response file and logon script configuration file**

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

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

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

### Table 31. Windows agent installation parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Argument</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Setup: type</td>
<td><code>SetupType</code></td>
<td>Typical</td>
</tr>
<tr>
<td></td>
<td><strong>Description</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Select Typical</strong> to install the agent using default values for most of the parameters except <code>MessageHandlerAddress</code> which you must specify. Select <strong>Custom</strong> if you want to customize other parameters.</td>
<td></td>
</tr>
<tr>
<td>Agent configuration: Scan group name</td>
<td><code>ScanGroup</code></td>
<td><strong>DEFAULT</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Description</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>The name of the scan group to which the agent will belong. The name cannot contain any special characters (e.g. spaces).</td>
<td></td>
</tr>
<tr>
<td>Parameter</td>
<td>Argument</td>
<td>Default</td>
</tr>
<tr>
<td>-----------</td>
<td>----------------</td>
<td>---------</td>
</tr>
<tr>
<td><strong>Message handler address</strong></td>
<td>MessageHandlerAddress</td>
<td>localhost</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Specify the hostname or IP address of the Tivoli Asset Discovery for Distributed server. Message handler is a server component which manages incoming and outgoing agent data.</td>
</tr>
<tr>
<td><strong>Port</strong></td>
<td>Port</td>
<td>9988</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Specify the port number used by the agent. This value is used for nonsecure communications (SecurityLevel=0).</td>
</tr>
<tr>
<td><strong>Secure port</strong></td>
<td>SecureAuth</td>
<td>9999</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Specify the port number used by the agent. This value is used for secure communications with server authentication (SecurityLevel=1).</td>
</tr>
<tr>
<td><strong>Client Auth Secure Port</strong></td>
<td>SecureAll</td>
<td>9977</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Specify the port number used by the agent. This value is used for secure communications with client and server authentication (SecurityLevel=2).</td>
</tr>
<tr>
<td><strong>Agent temporary path</strong></td>
<td>AgentTempPath</td>
<td>YourTempDir\tlm</td>
</tr>
<tr>
<td></td>
<td></td>
<td>To override the location where the agent keeps the working files, enter a valid path.</td>
</tr>
<tr>
<td><strong>Agent destination path</strong></td>
<td>CITInstallPath</td>
<td>C:\Program Files\Tivoli\cit</td>
</tr>
</tbody>
</table>
| | | Specify the Common Inventory Technology installation folder.  
**Important:** Note that the Common Inventory Technology installation folder cannot be the same as or located inside the agent installation folder.  
**Note:** If there is already an instance of Common Inventory Technology installed on the system, this parameter will be ignored and the agent will use the existing installation of Common Inventory Technology. If the existing version of Common Inventory Technology is older, it will be upgraded during the agent installation. |
| **Security level** | SecurityLevel | 0 |
| | | Determines the level of security to be used for communication between the agent and the Tivoli Asset Discovery for Distributed server. Possible values are:  
0 To use nonsecure communication.  
1 To use secure communications with server authentication.  
2 To use secure communications with client and server authentication.  
**Note:**  
1. The Tivoli Asset Discovery for Distributed server configured for maximum security can communicate with agents set to maximum security only. If the server is configured to use medium security, only agents set to medium or maximum security can connect to it. The server configured for minimum security can support agents set for any security level.  
2. If you select medium (1) or maximum (2) security, you must perform a series of tasks to set up and install certificates. For full information about enabling security, see the "Security" section of the Tivoli Asset Discovery for Distributed infocenter. |
| **FIPS enabled** | FipsEnabled | n |
| | | Specifies whether the agent is to use FIPS-approved modules in the communication of encrypted data. Possible values are \textit{y} (yes) and \textit{n} (no). |
Table 31. Windows agent installation parameters (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Argument</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agent configuration: Use proxy</td>
<td>UseProxy</td>
<td>n</td>
<td>Specifies whether the Tivoli Asset Discovery for Distributed server is protected by a proxy server. The following values are permitted: y The Tivoli Asset Discovery for Distributed server is protected by a proxy server. n The Tivoli Asset Discovery for Distributed server is not protected by a proxy server.</td>
</tr>
<tr>
<td>Agent configuration: Proxy address</td>
<td>ProxyAddress</td>
<td></td>
<td>If UseProxy is set to y, enter the address (host name or IP address) of the proxy server.</td>
</tr>
<tr>
<td>Agent configuration: Proxy port</td>
<td>ProxyPort</td>
<td>3128</td>
<td>If UseProxy is set to y, enter the port of the proxy server.</td>
</tr>
<tr>
<td>Digital certificate: Install certificate</td>
<td>InstallServerCertificate</td>
<td>n</td>
<td>If you have selected SecurityLevel=1 or SecurityLevel=2, you can choose to install the server certificate. The possible values are y (yes) and n (no). See the ServerCustomSSLCertificate and ServerCertFilePath description below.</td>
</tr>
<tr>
<td>Digital certificate: Server custom certificate</td>
<td>ServerCustomSSLCertificate</td>
<td>n</td>
<td>If you have selected to supply the server certificate (installServerCertificate=y), you can choose to provide your own server certificate to be used by the agent for secure communications with the server. The permitted values are: y Indicates that you want to provide your own server certificate. n Indicates that you want to use the server test certificate. Note: The server test certificate can only be used for test purposes. Obtain your own certificate if secure communication is required in a live environment. If you select the value true, you must also supply the certificate pathname (ServerCertFilePath).</td>
</tr>
<tr>
<td>Digital certificate: Server certificate pathname</td>
<td>ServerCertFilePath</td>
<td></td>
<td>If you have selected to supply a server certificate (ServerCustomSSLCertificate=y), you must provide the pathname and filename of your own server certificate. The name of the certificate must be cert.arm. If the path contains spaces, enclose the whole path in double-quotes.</td>
</tr>
<tr>
<td>Digital certificate: Agent certificate pathname</td>
<td>AgentCertFilePath</td>
<td></td>
<td>Provide the path name and filename of the agent certificate in order to add a new agent to the server with enabled MAX security level. The name of the certificate must be key.kdb. If the path contains spaces, enclose the whole path in double-quotes.</td>
</tr>
</tbody>
</table>

UNIX agents installation response file

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

Note: Do not use the # character in any of the agent parameters. Parameter values cannot include spaces or UTF strings.
You can find the response file in the following location: /etc/response_file.txt.

Table 32. UNIX agents installation parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Argument</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Port</td>
<td>Port</td>
<td>9988</td>
</tr>
<tr>
<td>Specify the port number used by the agent. This value is used for nonsecure communications (SecurityLevel=0).</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Secure Port</td>
<td>SecureAuth</td>
<td>9999</td>
</tr>
<tr>
<td>Specify the port number used by the agent. This value is used for secure communications with server authentication (SecurityLevel=1).</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Client Auth Secure Port</td>
<td>SecureAll</td>
<td>9977</td>
</tr>
<tr>
<td>Specify the port number used by the agent. This value is used for secure communications with client and server authentication (SecurityLevel=2).</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Agent configuration: Agent Temporary Path</td>
<td>AgentTempPath</td>
<td>/tmp/itlm</td>
</tr>
<tr>
<td>To override the location where agent keeps the working files, enter a valid path.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Agent configuration: Message Handler Address</td>
<td>MessageHandlerAddress</td>
<td>localhost</td>
</tr>
<tr>
<td>Specify the hostname or IP address of the Tivoli Asset Discovery for Distributed server. Message handler is a server component which manages incoming and outgoing agent data.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Agent configuration: Scan Group Name</td>
<td>ScanGroup</td>
<td>DEFAULT</td>
</tr>
<tr>
<td>The name of the scan group to which the agent belongs. The agent can be reassigned to another scan group by the Tivoli Asset Discovery for Distributed server, or by the inventory administrator on the server. The name of the scan group cannot contain any special characters (e.g. spaces).</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Agent configuration: Security level</td>
<td>SecurityLevel</td>
<td>0</td>
</tr>
<tr>
<td>Determines the level of security to be used for communication between the agent and the Tivoli Asset Discovery for Distributed server. Possible values are:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>0</td>
<td>To use unsecure communication.</td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>To use secure communications with server authentication.</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>To use secure communications with client and server authentication.</td>
<td></td>
</tr>
<tr>
<td>Note:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1. The Tivoli Asset Discovery for Distributed server configured for maximum security can communicate with agents set to maximum security only. If the server is configured to use medium security, then only agents set to medium or maximum security can connect to it. A server configured for minimum security can support agents set for any security level.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2. If you select medium (1) or maximum (2) security, you must perform a series of tasks to set up and install certificates. For full information about enabling security, see the &quot;Security&quot; section of the Tivoli Asset Discovery for Distributed infocenter.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Agent configuration: Use Proxy</td>
<td>UseProxy</td>
<td>n</td>
</tr>
<tr>
<td>Specifies whether the Tivoli Asset Discovery for Distributed server is protected by a proxy server. The following values are permitted:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>y</td>
<td>The Tivoli Asset Discovery for Distributed server is protected by a proxy server.</td>
<td></td>
</tr>
<tr>
<td>n</td>
<td>The Tivoli Asset Discovery for Distributed server is not protected by a proxy server.</td>
<td></td>
</tr>
</tbody>
</table>
Table 32. UNIX agents installation parameters (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Argument</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Agent configuration: Proxy Port</td>
<td>ProxyPort</td>
<td></td>
</tr>
<tr>
<td>If UseProxy is y, enter the port of the proxy server.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Agent configuration: Proxy Address</td>
<td>ProxyAddress</td>
<td></td>
</tr>
<tr>
<td>If UseProxy is y, enter the address (host name or IP address) of the proxy server.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Agent configuration: FIPS Enabled</td>
<td>FipsEnabled</td>
<td>n</td>
</tr>
<tr>
<td>Specifies whether the agent is to use FIPS-approved modules in the communication of the encrypted data. The possible values are y (yes) and n (no).</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Agent configuration: CIT Destination Path</td>
<td>CITInstallPath</td>
<td></td>
</tr>
<tr>
<td>Specify the Common Inventory Technology installation folder.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Important: Note that the Common Inventory Technology installation folder cannot be the same as or located inside the agent installation folder.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Note: If there is already an instance of Common Inventory Technology installed on the system, this parameter will be ignored and the agent will use the existing installation of Common Inventory Technology. If the existing version of Common Inventory Technology is older, it will be upgraded during the agent installation.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Digital certificate: Install server certificate</td>
<td>InstallServerCertificate</td>
<td>n</td>
</tr>
<tr>
<td>If you have selected SecurityLevel=1 or SecurityLevel=2, you can choose to install the server certificate. Possible values are y (yes) and n (no). See the ServerCustomSSLCertificate and ServerCertFilePath descriptions below.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Digital certificate: server custom certificate</td>
<td>ServerCustomSSLCertificate</td>
<td>n</td>
</tr>
<tr>
<td>If you have selected to supply the server certificate (InstallServerCertificate=y), you can choose to provide your own server certificate to be used by the agent for secure communications with the server.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>The permitted values are:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>y Indicates that you want to provide your own server certificate.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>n Indicates that you want to use the server test certificate.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Note: The server test certificate can only be used for test purposes. Obtain your own certificate if secure communication is required in a live environment.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>If you select the value y, you must also supply the certificate pathname (ServerCertFilePath).</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Digital certificate: server certificate pathname</td>
<td>ServerCertFilePath</td>
<td></td>
</tr>
<tr>
<td>If you have selected to supply a server certificate (ServerCustomSSLCertificate=y), you must provide the pathname and filename of the certificate. The name of the certificate must be cert.arm. If the path contains spaces, enclose the whole path in double-quotes.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Linux 390: Node capacity</td>
<td>SystemActiveProcessors</td>
<td></td>
</tr>
<tr>
<td>If the Linux 390 image is running on IFL processors, this is the total number of IFL processors in the CEC. If the image is running on CP processors, this is the total number of CP processors in the CEC. This parameter is required for the installation to succeed.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Linux 390: Shared pool capacity</td>
<td>SharedPoolCapacity</td>
<td></td>
</tr>
<tr>
<td>If the Linux 390 image is configured to share processors, specify the total number of shared processors in the CEC. Enter 0 if no shared processors are used by this image. This parameter is required for the installation to succeed. The value of this parameter cannot exceed the value of SystemActiveProcessors.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Parameter</td>
<td>Argument</td>
<td>Default</td>
</tr>
<tr>
<td>-----------------------------------</td>
<td>----------------</td>
<td>---------</td>
</tr>
<tr>
<td>Description</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Linux 390: Processor type</td>
<td>ProcessorType</td>
<td>IFL</td>
</tr>
<tr>
<td>Specify the type of processors the Linux image is running on. The possible values are:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CP</td>
<td>Your Linux image is running on CP processors.</td>
<td></td>
</tr>
<tr>
<td>IFL</td>
<td>Your Linux image is running on IFL processors.</td>
<td></td>
</tr>
<tr>
<td>This parameter is required for the installation to succeed.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Linux 390: MachineType</td>
<td>MachineType</td>
<td>z9</td>
</tr>
<tr>
<td>Specify the type of physical machine Linux 390 is running on. The possible values are:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>z9</td>
<td>If you are installing the agent on any machine older than z10 e.g. system z9, z90, or S/390.</td>
<td></td>
</tr>
<tr>
<td>z10</td>
<td>If you are installing the agent on a z10 or z196 server computer.</td>
<td></td>
</tr>
<tr>
<td>Solaris OS: Installation on Dynamic Domain</td>
<td>InstallOnDD</td>
<td>n</td>
</tr>
<tr>
<td>If the agent is being installed on Dynamic Domain, this value should be set to true, otherwise to false. The permitted values are:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>y</td>
<td>indicates that the agent is being installed on Dynamic Domain</td>
<td></td>
</tr>
<tr>
<td>n</td>
<td>Indicates that the agent is not being installed on Dynamic Domain</td>
<td></td>
</tr>
<tr>
<td>Disable Rollback</td>
<td>disableRollBack=y</td>
<td></td>
</tr>
<tr>
<td>Add this parameter to the response file to disable the automatic rollback of changes to the system in case of a failed installation. This preserves the failed installation on your computer, and allow you to examine it to discover the reasons for the failure.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Digital certificate: Agent certificate path name</td>
<td>AgentCertFilePath</td>
<td></td>
</tr>
<tr>
<td>Provide the path name and filename of the agent certificate in order to add a new agent to the server with enabled MAX security level. The name of the certificate must be key.kdb. If the path contains spaces, enclose the whole path in double-quotes.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**IBM i agent installation response file**

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

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

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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Argument</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Agent configuration: Port</td>
<td>Port</td>
<td>9988</td>
</tr>
<tr>
<td>Specify the port number used by the agent. This value is used for nonsecure communications (SecurityLevel=0).</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Parameter</td>
<td>Argument</td>
<td>Default</td>
</tr>
<tr>
<td>---------------------------</td>
<td>---------------</td>
<td>---------</td>
</tr>
<tr>
<td><strong>Agent configuration: Port</strong></td>
<td><strong>SecureAuth</strong></td>
<td>9999</td>
</tr>
<tr>
<td>Description</td>
<td>Specify the port number used by the agent. This value is used for secure communications with server authentication (\text{SecurityLevel}=1).</td>
<td></td>
</tr>
<tr>
<td><strong>Agent configuration: Port</strong></td>
<td><strong>SecureAll</strong></td>
<td>9977</td>
</tr>
<tr>
<td>Description</td>
<td>Specify the port number used by the agent. This value is used for secure communications with client and server authentication (\text{SecurityLevel}=2).</td>
<td></td>
</tr>
<tr>
<td><strong>Agent configuration: Message Handler Address</strong></td>
<td><strong>MessageHandlerAddress</strong></td>
<td></td>
</tr>
<tr>
<td>Description</td>
<td>Specify the hostname or IP address of the Tivoli Asset Discovery for Distributed server. Message handler is a server component which manages incoming and outgoing agent data. This is a mandatory parameter.</td>
<td></td>
</tr>
<tr>
<td><strong>Agent configuration: Scan Group Name</strong></td>
<td><strong>ScanGroup</strong></td>
<td>DEFAULT</td>
</tr>
<tr>
<td>Description</td>
<td>The name of the scan group to which the agent will belong. The agent may be reassigned to another scan group by the Tivoli Asset Discovery for Distributed server, or by the inventory administrator on the server.</td>
<td></td>
</tr>
<tr>
<td><strong>Agent configuration: Security level</strong></td>
<td><strong>SecurityLevel</strong></td>
<td>0</td>
</tr>
</tbody>
</table>
| Description               | Determines the level of security to be used for communication between the agent and the Tivoli Asset Discovery for Distributed server. Possible values are:  
0 To use nonsecure communication.  
1 To use secure communications with server authentication.  
2 To use secure communications with client and server authentication.  
\textbf{Note:}  
1. The Tivoli Asset Discovery for Distributed server configured for maximum security can communicate with agents set to maximum security only. If the server is configured to use medium security, then only agents set to medium or maximum security can connect to it. A server configured for minimum security can support agents set for any security level.  
2. If you select medium (1) or maximum (2) security, you must perform a series of tasks to set up and install certificates. For full information about enabling security, see the "Security" section of the Tivoli Asset Discovery for Distributed infocenter. |
| **Agent configuration: Use Proxy** | **UseProxy** | n       |
| Description               | Specifies whether the Tivoli Asset Discovery for Distributed server is protected by a proxy server. The following values are permitted:  
y The Tivoli Asset Discovery for Distributed server is protected by a proxy server.  
n The Tivoli Asset Discovery for Distributed server is not protected by a proxy server. |
| **Agent configuration: Proxy Port** | **ProxyPort** |         |
| Description               | If \text{UseProxy} is \text{y}, enter the port of the proxy server. |
| **Agent configuration: Proxy Address** | **ProxyAddress** |         |
| Description               | If \text{UseProxy} is \text{y}, enter the address (host name or IP address) of the proxy server. |
Table 33. IBM i agents installation parameters (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Argument</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Digital certificate: Install certificate</td>
<td><strong>InstallServerCertificate</strong></td>
<td><strong>n</strong></td>
</tr>
<tr>
<td><strong>Description</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>If you have selected <strong>SecurityLevel=1</strong> or <strong>SecurityLevel=2</strong>, you can choose to install certificates. Possible values are:</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>y</strong> Install the server certificate defined in <strong>ServerCertFilePath</strong> or agent certificate defined in <strong>PrivateServerCertFilePath</strong>, or both. If <strong>ServerCertFilePath=none</strong>, the server test certificate will be installed.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>n</strong> Do not install any certificate file.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Digital certificate: server certificate path name**

<table>
<thead>
<tr>
<th>ServerCertFilePath</th>
</tr>
</thead>
</table>

If you have selected to supply certificates (**installServerCertificate=y**), you can choose to provide your own server certificate to be used for server authentication by the agent (**SecurityLevel>0**).

Possible values are:

- **path/cert.arm** - Indicates that you want to provide your own server certificate.
- **none** - Indicates that you want to use the server test certificate.

The name of the server certificate must be **cert.arm**. If the path contains spaces, enclose the whole path in double-quotes.

**Note:** The test certificate may only be used for test purposes as it is in the name of IBM and is insecure (the same certificate is distributed to all customers).

**Digital certificate: agent certificate path name**

<table>
<thead>
<tr>
<th>PrivateCertFilePath</th>
<th>none</th>
</tr>
</thead>
</table>

If you have selected to supply SSL certificates (**installServerCertificate=y**), you can provide the path name of your agent certificate file to be used for client authentication by the server (**SecurityLevel=2**). If the path contains spaces, enclose the whole path in double-quotes.

**Troubleshooting agent installation and uninstallation**

Find out more about common problems that might occur during agent installation, uninstallation, or upgrade and their solutions.

**Agent installation problems on AIX platforms**

When installing the agent on an AIX machine, you may encounter one of the common installation problems. Find the description that matches your problem and solve it.

The list below contains common agent installation problems on AIX:

**On AIX, the native installer hangs after installation. The agent is installed successfully, but the status is not changed to success. The following message is displayed:** Some entries in the next screen do not have the correct string length. Check your language environment variable and the code set.

This error occurs when the packages **bos.loc.com.utf** and **bos.loc.utf.EN_US** are installed on the system, and the **LANG** environmental variable is set to **EN_US**.
Change the value of the `LANG` variable in `/etc/environment` from `EN_US` to `en_US`, or type `LANG=en_US` to change the value for the current session only.

On AIX, after upgrading the server from version 7.1 to 7.2 or 7.2.2, you may experience a situation when the agent version 7.1 stops sending scheduled software scans.

To solve this problem, stop the agent, delete its cache and start the agent.

If an agent running in an AIX 6.1 logical partition (LPAR) is upgraded to version 7.2.2 using Tivoli Configuration Manager or self-update method, it might be impossible to install version 7.2.2 agents in workload partitions (WPARs) created in the logical partition (LPAR).

There are two ways to install the agent in a workload partition:

- Reininstall the agent in the logical partition using native installation method and then install agents in workload partitions using native installation methods, too.

- Do not change the configuration of the agent installed in the logical partition but perform the installation in workload partition paying special attention to the paths in the response file. To install the agent in a workload partition, perform the installation in the same way as in the logical partition but provide all paths in the response file, ensuring that no directory that is shared with global AIX is read only. In particular, Common Inventory Technology installation directory needs to be modified since the default is located under the `/opt` directory, which for default workload partition is set to read only.

When installing an agent, the following message displays: "CODAG099E Installing of the Common Inventory Technology (CIT) infrastructure element SPB has failed. Installation cit failed".

To find out more, run the following command: `INSTALL_PATH/utilities/cit/wcitinst i 5724-D33 -s INSTALL_PATH/asures/cit/cit.spb -d CIT_INSTALL_PATH`

where the default Common Inventory Technology installation path is `/opt/tivoli/cit`

Uninstallation is successful, but GSKit directory is still in use by an LPAR process, and can not be removed.

After removing an agent from a workload partition (WPAR), the GSKit directory on the WPAR still exists, which means that a file cannot be removed from the WPAR directory. To remove the file, restart the WPAR.

**Agent installation problems on Linux operating system**

Solve the problems that you may encounter during agent installation on Linux platforms.

Find the description that matches your problem and follow the instructions to solve it:

**The installation wizard hangs when installing on Linux platforms.**

When a prerequisite for the Java Virtual Machine (JVM) that is bundled with the installation package is missing, check the prerequisites for the JVM on that platform. When you launch the set up file, a Java Runtime Environment (JRE) is installed that is needed by the wizard. Some environmental settings or fix packs might be required to enable the JRE function correctly. Refer to the following information for details of settings and fix packs that are required on each platform:
Agent installation fails on Red Hat Enterprise Linux version 4. The agent installation fails and in the install agent trace the following error is displayed:

```
wdinstsp: error while loading shared libraries: libstdc++.so.5: cannot open shared object file: No such file or directory.
```

Install the following compatible library package:
```
compat-libstdc++-33-3.2.3-47.3.i386.rpm
```

Agent installation fails on Linux 390 platforms with the error -8 in the log file `/tmp/manualDeploy/tmp_dir/slmrc` and in the trace file, the following entry appears: `<LogText><![CDATA[WizardException: (error code = 200; message="Unable to find success string in the log file: /tmp/manualDeploy/tmp_dir/slmrc")]]&gt;</LogText>`.

Verify that you entered the correct values for Shared pool capacity and Active processors.

The agent does not start on Linux systems (such as zLinux) and the following message appears: **CODAGO016E - An error occurred starting the agent.**

Check for messages like the following: SELinux is preventing `/opt/tivoli/cit/bin/wscancfg` from loading `/opt/tivoli/cit/bin/libbase.so` which requires text relocation. You can find SELinux logs in the `syslog` in `/var/log/messages`. To view complete SELinux messages, run the following command:
```
sealert -l d601071f-34fe-4ef4-ad97-2dada2900635
```

This error occurs when your Linux operating system is in `Enforcing` mode. You must change the mode to `Permissive` or `Disabled` before you install the agent. To do so, set the parameter `SELINUX` in the file `/etc/selinux/config` to `permissive` or to `disabled`. You cannot set the security setting back to `Enforcing`; if you do so the agent will stop working. `Enforcing` mode may be preserved if you decide to change the file context to `textrel_shlib_t` for all the libraries used by agent using the command:
```
chcon -t textrel_shlib_t /path_to_lib/libname.so
```

Although the installation on an agent fails, the system reports a successful installation.

When the problem occurs, complete the following steps:

1. Execute the following uninstallation command:
   ```
   rpm -e ILMT-TAD4D-agent
   ```

2. If the uninstallation fails, use the command:
   ```
   rpm -e --noscripts ILMT-TAD4D-agent
   ```

3. If the target directory for the agent has been created, delete it.

4. If there are is an `/etc/tlmagent.ini` file left, delete it.

When installing an agent, the following message displays: "**CODAG099E** Installing of the Common Inventory Technology (CIT) infrastructure element SPB has failed. Installation cit failed".

To find out more, run the following command:
```
INSTALL_PATH/utilities/cit/wcinitst i 5724-D33 -s INSTALL_PATH/utilities/cit/cit.spb -d CIT_INSTALL_PATH
```

where the default Common Inventory Technology installation path is `/opt/tivoli/cit`
Installation of agent fails on Security-Enhanced Linux and the following message displays: "/var/itlm/gskit/bin/gsk7ver: error while loading shared libraries: /var/itlm/gskit/lib/libgsk7krsw.so: cannot restore segment prot after reloc: Permission denied".

GSKit binary files cannot run in SE Linux, for example /var/itlm/gskit/bin/gsk7ver, if text relocation is turned on. To turn off the checking of text relocation in GSKit packages run the following commands after changing to the agent directory:

```
setsebool -P allow_execmod=1
./tlmagent -g
```

**Agent installation problems on IBM i, Windows and Solaris platforms**

Solve the problems that may occur during agent installation.

Follow the instructions to solve the problem that you have encountered:

**The agent install wizard for IBM i displays message CODIN0099E, indicating that the agent cannot be installed. This message states that an agent is already installed on the computer**

On IBM i platforms, you must uninstall the agent before re-installing it. If the objective of the new installation is to change the agent parameters, before you reinstall you must also manually remove the configuration file from the path: /QIBM/UserData/QITLM/conf.

When you reinstall the agent, a new agent ID is generated, so previous information collected by the agent on the computer is not included in any reports for the new agent. The entry for the old agent is still present in the server database and cannot be immediately deleted. Agents must be recognized by the administration server as inactive before they can be deleted. When the agent status changes to inactive, you can delete it.

**Unable to uninstall the agent (manual Websphere Application Server installation used) on computers running Windows Vista (32 bit). The agent does not appear in the Programs to remove list.**

Uninstall the agent with the tlmuninst script. See the *Installation Guide* for details.

**When installing an agent on Solaris using native installers, the following message is displayed: WARNING: The <depends> package "SUNWcsu Core Solaris, (Usr)" is a prerequisite package and should be installed.**

It does not mean that the prerequisite is not installed, but that an element required during the agent installation is being checked.

**When installing an agent on Windows or Solaris, the following message displays: "CODAG099E Installing of the Common Inventory Technology (CIT) infrastructure element SPB has failed. Installation cit failed".**

To find out more, run the following command:

- on Solaris, `INSTALL_PATH/Utilities/cit/wcitinst i 5724-D33 -s INSTALL_PATH/Utilities/cit/cit.spb -d CIT_INSTALL_PATH`
  where the default Common Inventory Technology installation path is: `/opt/tivoli/cit`
- on Windows, `INSTALL_PATH\Utilities\cit\wcitinst.exe i 5724-D33 -s INSTALL_PATH\Utilities\cit\cit.spb -d CIT_INSTALL_PATH`
  where the default Common Inventory Technology installation path is:
    - on Windows `C:\Program Files\Tivoli\cit`
Installation of an agent on Windows fails and the following message can be found in the trace file: OnError: Error 1606. Could not access network location "<path>".

This problem occurs because of quotation marks in the installation path. When defining the path, use the following example:

ILMT_INSTALL_PATH=C:\Program files\ilmt

Agent upgrade and self-update problems

Solve the problems that may occur during the agent upgrade or self-update process.

The list below contains descriptions of common agent problems. Find the description that matches the problem you encountered and follow the instructions to solve it:

**After upgrading the server, it is not able to answer the requests made by the agent.** Upgrade the agent manually.

**On Windows, the agent self-update fails with the -510 return code.**

Check if the `<agent_temp_dir>` path located in the `tlmagent.ini` file includes some spaces. If it does, modify the path so that it does not include any spaces, and restart the agent.

**On bare metal Solaris 10, the agent self-update cannot be performed on V7.2 agents.**

If you experience the problem, restart the agent. After the agent is restarted, self-update should be performed successfully.

**Following automatic self-update on Windows platforms, the agent does not restart automatically.**

The agent does not restart because a reboot of the computer is needed to load libraries required by the corequisite GSkit software.

**Agent self-update fails because a security certificate cannot be added to the agent keystore.**

Agent self-update can be triggered by a change to the agent itself of a change to its security certificate. If the update is required because of a changed certificate you must ensure that the certificate has not already been changed on the current date. When certificates are automatically imported into the keystore the day, month, and year of the import is assigned as the unique ID of the certificate, so only a single import can be allowed on any one day.

**While upgrading agents on Linux, a file conflict error is displayed.**

The error occurs when you use the command with the `-ihv` parameter. To solve the problem, you need to use the `-Uhv` parameter as shown in Upgrading V7.2 agents (installed natively) using native installers

Other agent installation problems

Find the solution to problems that you encountered during agent installation.

Choose the description that matches the problem that occurred when you were installing the server and follow the instructions to solve it.
Agent files cannot be downloaded.
This is a network connectivity problem that can be caused by an unusually high amount of traffic or by an agent installation tool error. Wait for a short time and then retry the operation. If the problem persists, report the problem to the system administrator. Try deploying the agent from a different machine.

No status is returned to the server.
Check that the agent has been installed on the node. On Windows, you can open the services panel from the control panel and check for the agent. On UNIX, enter the following command: `ps -ef | grep tlmagent`. If the agent is running a response is returned. If it is not, there is no response. Also check the `slmrc` file for the return code.

A certificate for secure communications is not added to the keystore.
This happens if a certificate has already been added to the keystore on the same day. Only one certificate can be added automatically on any one day. You can either add the certificate manually using the keystore utilities or wait until the following day for the automatic update to be performed. Run the following command: `setagentconf -s active`.

Agent installation fails if the agent was previously installed and uninstalled.
In order to do a fresh installation of agent the following files and directories must be deleted prior to the installation:

- `/etc/itlmagent.ini`
- `/var/itlm/`

File paths and names can differ in case of custom installation.

You cannot put the focus in entry fields using Cygwin/X as a remote X-server after displaying the modal window. This happens when you forget to enter server information during the install and you try advance to the next screen. An error message tells you that you must enter server information, but then you will not be able to put the focus of the cursor in any text fields.

To solve this problem, launch the X-server using the `Cygwin/X startx` command as it is suggested at the following link: [http://x.cygwin.com/docs/ug/using.html](http://x.cygwin.com/docs/ug/using.html)

The agent cannot be uninstalled by system native installation tools after it has been upgraded from version 2.3 or 7.1 to 7.2 or 7.2.2 using Tivoli Configuration Manager or the self-update method. System registry is not updated.
On an agent upgraded in this way a refresh installation using native installation method can be performed. In this case, system registry will be updated. After that, you can uninstall the agent using the `tlmunins.sh` script.

Agent native installation fails, either during the preinstallation or postinstallation phase.
The process of installing agents natively consists of three phases:
1. Preinstallation
2. Installation (copying of files)
3. Postinstallation (configuration)

If the installation fails during the first phase, you might get the following error message:

```
Preparing... ########################################### [100%]
error: %pre(ILMT-TAD4D-agent-7.2.2-1.i386) scriptlet failed, exit status exit_code
```
If the installation fails during the third phase, you might get the following error message:

Preparing... ########################################### [100%]

error: %post(ILMT-TAD4D-agent-7.2.2-1.i386) scriptlet failed, exit status exit_code

You need to rerun the agent installer. For information how to do it see [Rerunning a failed agent installation](#).

### Installing of agents in bulk using customer-specific tools fails.

One of the possible reasons why this happens is because the customer-specific tools that deploy agents on a large number of computers set the value in the `current_working_directory` parameter to `null` (when running a new process on an endpoint). To prevent agent installation failures set the value to `non-null` (when possible).

### Agent native installation fails because of missing Global Security Toolkit prerequisite.

To check what prerequisites are missing, run the following script:

```
agent_install_path/gskit/private_checkinstall
```

You should get listing similar to the one below:

```
Required Patch 108435-14 missing
Required Patch 111327-05 found
Required Patch 108991 found
Required Patch 108993-31 found
Required Patch 108528-29 found
Required Patch 113648-03 found
Required Patch 116602-01 found
Required Patch 111317-05 found
Required Patch 111023-03 found
Required Patch 115827-01 found
```

Search your operating system vendor's Web site and download the patch (in the example above 108435-14). Install the patch and rerun the agent native installation.

### Agent installation fails because of incorrect Common Inventory Technology installation directory.

Common Inventory Technology cannot be installed in the agent installation directory. If the value of the `CITInstallPath` parameter in the agent installation response file specifies an installation directory the same as or located inside the agent installation directory, the agent installation fails. If your agent installation or upgrade fails due to this problem, uninstall the old agent and install the newer version from scratch.

### Disabling rollback of failed agent installations

When the installation of an agent is not successful, any changes that have been made to the target computer by the failed installation process are rolled back, leaving the environment ready for a fresh installation. On Windows and UNIX platforms you can disable this feature so that the failed installation is not removed from the target computer.

Disabling rollback allows you and IBM support to investigate the state of the installation at the point when it failed. This is useful if you are unable to identify the source of the problem from either the return code or the FFDC.

**Note:** On IBM i platforms rollback is disabled by default. Note also that if you use native installers, on AIX and Windows, the system registry is cleaned up no matter what the `disableRollBack` value is.
Procedure
1. On Windows platforms, type the following command into the system command prompt: set disableRollBack=yes.
2. On UNIX platforms, add the following line to the agent installation response file at agent installation: disableRollBack=yes.
Chapter 4. Uninstalling

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

Uninstalling the Tivoli Asset Discovery for Distributed servers and databases

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

You must uninstall the product before you can install it again on the same computer. Removing the files or dropping the database is not enough to complete the installation.

If you are uninstalling the database element to move it to a different computer and you want to retain the data held in the database, make a backup of the database before uninstalling. Then, restore the backup to populate the database that you have installed on the new computer. See “Moving the TLMA database to a separate server” on page 61 for more information.

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

Uninstalling the server in interactive mode

Use the uninstallation wizard to specify the parameters for the uninstallation step by step.

Before you begin

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

To do this:

- The uninstall wizard is located in the folder INSTALL_DIR\uninst. On UNIX platforms, there is a directory called Uninstall. This directory is not the uninstall folder. It contains files used in the uninstallation.

Procedure

1. Start the uninstall wizard (Windows) or uninstaller.sh (UNIX).
   a. Select the Add/Remove Programs option from the Control Panel.
   b. Select IBM Tivoli Asset Discovery for Distributed.
   c. Click Remove.
2. On the welcome screen, click Next to start uninstallation.
3. The wizard detects the elements that are present on the computer. Deselect any that you do not wish to uninstall. Leave the option to drop the TLMA database selected if appropriate.
If an error is generated when attempting to drop the database, you can manually drop the database using the DB2 command `db2 drop database tlma`, where `tlma` is the name of the Tivoli Asset Discovery for Distributed database.

4. Click Next. The wizard displays a panel showing the elements to be uninstalled. Click Next to continue with the uninstallation.

5. When the uninstallation is complete, the uninstaller lists all the completed actions. Click Done to exit from the wizard.

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

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

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

**Uninstalling the server in silent mode**

When the uninstall wizard runs in silent mode, it uses the parameters provided in a response file.

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

The uninstall wizard is located in the folder `INSTALL_DIR\Uninstall`.

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

**Procedure**

1. Log on the computer where you want to run the wizard with Administrator or root rights.

2. Navigate to the `INSTALL_DIR\Uninstall` directory and open the `uninstallresponse.txt` file.

3. Edit the response file so that the parameters describe the uninstallation that you want to perform.

4. From the command-line interface, launch the wizard uninstall script (*uninstaller.exe* for Windows and *uninstaller.bin* for other platforms) with the following parameters:

   - **Linux**  
     ```bash
     uninstall.sh -f absolute_path_to_response_file -i silent
     ```

   - **Windows**  
     ```batch
     uninstall.bat -f absolute_path_to_response_file -i silent
     ```

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

The wizard does not uninstall the DB2 database, or delete any user group created during the DB2 installation. You need to delete these groups manually.
In order to delete the Tivoli Asset Discovery for Distributed logs you have to delete the contents of the Tivoli Common Directory (provided that no other IBM Tivoli application uses that folder to store its logs).

**The server and database uninstallation response file**
The `uninstallresponse.txt` file, which is provided with IBM Tivoli Asset Discovery for Distributed, is an InstallAnywhere options file. It defines arguments to set each parameter required by the Tivoli Asset Discovery for Distributed uninstallation wizard.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Parameter key name</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Shutting down all running processes to uninstall the Administration Server</td>
<td><code>RSP_AUTO_CLOSE_PROCESSES</code></td>
<td><code>true</code></td>
</tr>
<tr>
<td>Description</td>
<td>Specifies if the silent installer shuts down the running processes. To enable this option, uncomment the following line: <code>RSP_AUTO_CLOSE_PROCESSES=true</code></td>
<td></td>
</tr>
<tr>
<td>Note:</td>
<td>1. You do not need to specify this option to stop the server as the server stops automatically. 2. Only the processes that are recognized are shut down automatically.</td>
<td></td>
</tr>
<tr>
<td>Uninstalling the Tivoli Asset Discovery for Distributed server element</td>
<td><code>RSP_UNINSTALL_ADMIN</code></td>
<td><code>true</code></td>
</tr>
<tr>
<td>Specifies whether or not the Tivoli Asset Discovery for Distributed element should be uninstalled. The possible values are:</td>
<td><code>true</code> The server is uninstalled. <code>false</code> The server is not uninstalled.</td>
<td></td>
</tr>
<tr>
<td>This parameter is ignored if the server is not installed on the computer.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Uninstalling the Tivoli Asset Discovery for Distributed database element</td>
<td><code>RSP_UNINSTALL_ADMDB</code></td>
<td><code>true</code></td>
</tr>
<tr>
<td>Specifies whether or not the Tivoli Asset Discovery for Distributed Administration Server Database component should be uninstalled. Possible values are:</td>
<td><code>true</code> The database is uninstalled. <code>false</code> The database is not uninstalled.</td>
<td></td>
</tr>
<tr>
<td>This parameter is ignored if the element is not installed on the computer.</td>
<td>Note: You can uninstall the Administration Server Database component without dropping the TLMA database and deleting the tlmsrv user.</td>
<td></td>
</tr>
<tr>
<td>Uninstalling databases: drop database</td>
<td><code>RSP_UNINSTALL_TLMA</code></td>
<td><code>true</code></td>
</tr>
<tr>
<td>Specifies whether or not any Tivoli Asset Discovery for Distributed databases on this computer should be deleted. The possible values are:</td>
<td><code>true</code> The databases are dropped. <code>false</code> The databases are not dropped.</td>
<td></td>
</tr>
<tr>
<td>Removing the tlmsrv user</td>
<td><code>RSP_UNINSTALL_TLMSRV</code></td>
<td><code>true</code></td>
</tr>
<tr>
<td>Specify if the tlmsrv user account created on a target computer should be deleted. The possible values are:</td>
<td><code>true</code> The tlmsrv user should be removed. <code>false</code> The tlmsrv user should not be removed.</td>
<td></td>
</tr>
<tr>
<td>The bundled WebSphere Application Server user ID</td>
<td><code>RSP_TLM_WAS_ADMIN</code></td>
<td></td>
</tr>
</tbody>
</table>
### Running scripts to uninstall Tivoli Asset Discovery for Distributed

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

#### Before you begin

1. You need to have the `setupWAS.properties` file filled with the same parameters as those used during the deployment phase. See the topic *Editing the `setupWAS.properties` file*.
2. You need to have the following scripts and files in one directory, for example `WAS-scripts` directory:
   - `cleanupDataSources.jacl`
   - `cleanupServerSecurePorts.jacl`
   - `cleanupWAS.bat`
   - `cleanupWAS.sh`
   - `setupWAS.properties`
   - `undeployAdmin.jacl`
   - `undeployAdminCommon.jacl`
   - `undeployMessageHandler.jacl`

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

To do this:

#### Procedure

1. Open the command line prompt, and enter the directory which contains your installation scripts, for example `WAS-scripts`.
2. Run the following command with the path to the correct profile that you want to undeploy Tivoli Asset Discovery for Distributed from:

   ```script
   UNIX cleanupWAS.sh PATH_TO_THE_PROFILE [-f] [-l log_file_path] where -f continues on errors, and -l logs you into a given file (default log file: SetupWAS.log in current directory).
   ```

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

If the uninstallation fails, you can resume it by running the cleanupWAS.bat (Windows) or cleanupWAS.sh (Unix) script again with the -f (force) parameter.

3. After successfully undeploying the applications, restart the WebSphere Application Server.

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

**Scripts used in undeploying the server on WebSphere Application base version**

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

<table>
<thead>
<tr>
<th>Script file</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>undeployAdmin.jacl</td>
<td>The script uninstalls administration component.</td>
</tr>
<tr>
<td>undeployAdminCommon.jacl</td>
<td>The script uninstalls other files used by the administration component.</td>
</tr>
<tr>
<td>undeployMessageHandler.jacl</td>
<td>The script uninstalls the Message Handler component.</td>
</tr>
<tr>
<td>cleanupDataSources.jacl</td>
<td>The script deletes the JDBC Provider name.</td>
</tr>
<tr>
<td>cleanupServerSecurePorts.jacl</td>
<td>The script removes port numbers used for secure communication.</td>
</tr>
<tr>
<td>cleanupTimerManager.jacl</td>
<td>The script removes timer managers.</td>
</tr>
</tbody>
</table>

**Uninstalling agents**

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

**Before you begin**

**Important:** Do not put any files into agent installation directory - this directory should only contain agent files and data. Agent installation directory will be removed during uninstallation.

**Uninstalling Tivoli Asset Discovery for Distributed agents using the tlmunins script**

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

**Procedure**

1. Navigate to the directory where the agent is installed.
2. Run the uninstallation script.
   - On Windows, run tlmunins.bat.
   - On UNIX platforms, run tlmunins.sh.
If an agent was installed using native tools, the tlmunins script will automatically run an appropriate native tool to remove the agent.

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

**Uninstalling agents using native installation tools**

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

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

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

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

**Uninstalling AIX agents**

Uninstall AIX agents by using the `installp` command.

**Procedure**

1. Open the system command line.
2. To uninstall the agent, run one of the following commands depending on where the agent is installed.
   - If the agent is installed on an LPAR in the default location, run:
     \[ \text{installp} -u \text{ILMT-TAD4D-agent} \]
   - If the agent is installed on an LPAR in a custom location, run:
     \[ \text{installp} -R \text{usil\_custom\_location} -u \text{ILMT-TAD4D-agent} \]
   - Where `usil\_custom\_location` is the custom path where the agent is installed.
   - If the agent is installed on an LPAR and WPAR, run the following commands in the specified order.
     a. On a WPAR, run:
        \[ \text{installp} -u -Or \text{ILMT-TAD4D-agent} \]
     b. On an LPAR, run:
        \[ \text{installp} -u \text{ILMT-TAD4D-agent} \]

To complete the uninstallation, you must remove the agent in the administration console. See *Removing agents in the administration console*.

**Uninstalling HP-UX agents**

Uninstall HP-UX agents using the `swremove` command.

**Procedure**

1. Open a system command prompt.
2. Enter the following command:
   \[ \text{swremove} \text{ILMT-TAD4D-agent} \]

To complete the uninstallation, you need to remove the agent in the administration console. See *Removing agents in the administration console*.
Uninstalling IBM i agents
Uninstall IBM i agents using the IBM i function Delete Licensed Program.

Before you begin
Stop the agent before uninstallation.

Procedure
1. Open the system command line.
2. Enter the following command:
   ```
   DLTLPICPGM LICPGM(1IBMTLM)
   ```

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

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

Uninstalling Linux agents
Uninstall Linux agents using the rpm command.

Procedure
1. Open a system command prompt.
2. Enter the following command:
   ```
   rpm -e ILMT-TAD4D-agent-7.2.2
   ```

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

Uninstalling Solaris agents
Uninstall Solaris agents using the pkgrm command.

You can uninstall the agent in a global zone. If there are any agents installed in local zones set in this global zone, you need to uninstall them separately.

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

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

Uninstalling Windows agents
Uninstall Windows agents using the uninstallation wizard.

Procedure
1. Start the uninstall wizard.
   a. Select the Add/Remove Programs option from the Control Panel.
   b. Select ILMT-TAD4D Agent version 7.2.2.
c. Click **Remove**.

2. Click **OK** to commence the uninstallation.

3. When the uninstallation is completed, click **Finish** to exit from the wizard.

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

This information was developed for products and services offered in the U.S.A.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user’s responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785 U.S.A.

For license inquiries regarding double-byte character set (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan, Ltd.
1623-14, Shimotsuruma, Yamato-shi
Kanagawa 242-8502 Japan

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law:

INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION “AS IS” WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.
IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Corporation
2Z4A/101
11400 Burnet Road
Austin, TX  79758 U.S.A

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this information and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement, or any equivalent agreement between us.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

Trademarks

IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at "Copyright and trademark information" at www.ibm.com/legal/copytrade.shtml.

Adobe is a registered trademark of Adobe Systems Incorporated in the United States, and/or other countries.

IT Infrastructure Library is a registered trademark of the Central Computer and Telecommunications Agency which is now part of the Office of Government Commerce.

ITIL is a registered trademark, and a registered community trademark of the Office of Government Commerce, and is registered in the U.S. Patent and Trademark Office.
Intel, Intel logo, Intel Inside, Intel Inside logo, Intel Centrino, Intel Centrino logo, Celeron, Intel Xeon, Intel SpeedStep, Itanium, and Pentium are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.

Microsoft and Windows are trademarks of Microsoft Corporation in the United States, other countries, or both.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Java and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.
Index

**Special characters**

99

**A**

administration server
- uninstalling 145
administration server database
- moving 61
- uninstalling 145
agents
- bulk installing 122
- disabling SELinux 101
- failed installation
- disabling rollback 142
HACMP environments 92
hardware requirements
- disk space 88
HP-UX
- uninstalling 150
IBM i
- uninstalling 151
- installing 120
- native installers 104
- on AIX 105
- on HP-UX 109
- on IBM i 107
- on Linux 110
- on Windows 115
Windows logon scripts 126
Linux
- uninstalling 151
placement 16
- preparing certificates 96
product components 1
requirements 74
response files 129
software requirements 74, 86
Solaris
- uninstalling 151
uninstalling
- native installation tools 150
overview 145
tlmunins script 149
Windows 151
UNIX
- installation response files 131
virtualization considerations 85
Windows
- installation response files 129
AIX
- bulk installing agents 122
- uninstalling agents 150
authentication
- preparing agent certificates 96

**C**

capacity
- planning 16

certificates
- agents 96
CLI (command-line interface)
- components 1
clocks
- synchronizing 39
command-line interface (CLI)
- components 1
Common Inventory Technology enabler
- running 100
communications
- security 18
compatibility
- software requirements 74
components 1

data source for server
- configuring data source for server 62
- configuring in WebSphere Application Server 62
WebSphere Application Server 62
database
- installing
- interactive mode 40
databases
- agents 145
- moving to a different computer 61
- uninstalling 145
- user IDs 18
- disabling rollback 142

edited WebSphere Application Server
- installing
- interactive mode 40
- silent mode 53

files
- os400_agent.txt file
- IBM i agent 134
UNIX installation response
- editing 131
Windows installation response
- editing 129

H

HACMP (High Availability Cluster Multiprocessing)
support 92
Hardware and Software Identification for Distributed components 1

hardware requirements
- agents 74
- disk space for agents 88
- servers
  - disk space 10
  - memory and CPU 9
High Availability Cluster Multiprocessing (HACMP)
support 92
HP-UX
- bulk installing agents 122
- uninstalling agents 150

I

IBM i
- agents
  - uninstalling 151
- bulk installing agents 122
- language support 94
InstallAnywhere options file
- servers and databases
  - uninstall 147
installation
- access privileges 18
- agents
  - on AIX 105
  - on HP-UX 109
  - on IBM i 107
  - on Linux 110
  - on Windows 115
- Red Hat Linux 101
- Windows logon scripts 126
overview 3, 73
planning 4
response files 129
scenarios
- proof-of-concept 19
- security 103
server
- problems 62
servers
- response files 54
tasks 103
verifying servers 49, 57
WebSphere Application Server
- prerequisites 16
installation wizard
- installing agents
  - on Windows 115
installation wizards
- interactive uninstallation 145
InstallShield options file
- IBM i agent 134
Integrated Solutions Console
- verifying server installation 49, 57
interactive wizard
- uninstalling 145

© Copyright IBM Corp. 2002, 2010
L
language support
 IBM i agents 94
License Metric Tool
 components 1
Linux
  bulk installing agents 122
  security levels 18
  uninstalling agents 151
log files
  verifying installation 49, 57

M
move database 61

N
network
  planning 18

O
operating systems
  software requirements
    agents 74
options files
  IBM i agent 134
  os400_agent.txt file
    IBM i agent 134

P
patches
  software requirements
    agents 74
prerequisites
  language support for IBM i
    agents 94
privileges
  required for installation 18
  security levels 18

R
Red Hat Linux
  disabling SELinux 101
installation considerations 39
response files
  agents 129
  IBM i agent for silent installation 134
  servers and databases 147

S
scan groups 16
scripts
  removing Tivoli Asset Discovery for Distributed 148
  WebSphere Application Server 149
security
  levels 18
SELinux
  altering on Red Hat Linux 39

SELinux (continued)
  disabling on Red Hat Linux 101
server
  installing
    interactive mode 40
    problems 62
  silent mode 53
  uninstalling
    problems 62
server components
  placement 16
servers
  components 1
  hardware requirements
    CPU and memory 9
    disk space 10
  installing
    response files 54
  personal certificates
    generating 96
    removing 149
  response files 54
  uninstalling
    description 145
    overview 145
  verifying installation 49, 57
  service packs
    software requirements
      agents 74
      silent installation
        IBM i agent 134
      silent uninstallation
        servers 146
        using response files 147
    software considerations
      virtualization 85
    software distribution
      deploying agents 122
      software package blocks (SPBs)
        distributing in bulk 122
        parameters 123
    software requirements
      agents 74, 86
      Red Hat Linux 39
Solaris
  bulk installing agents 122
  uninstalling agents 151
  SPBs (software package blocks)
    distributing in bulk 122

T
Tivoli Asset Discovery for Distributed
  installation overview 1
  server installation planning 4
Tivoli Configuration Manager
  bulk installation 122
  tlmunins script
  uninstalling 149
topology
  planning 16

U
uninstallation
  agents
    native installation tools 150
    tlmunins script 149
databases 145
  IBM i agents 151
  server and database response file 147
  servers
    overview 145
    silent mode 146
  uninstalling
    server
      problems 62
UNIX
  disabling rollback 142

V
virtualization
  Common Inventory Technology enabler 100
  software considerations 85

W
WebSphere Application Server
  removing servers 149
  supported versions 16
Windows
  agents
    uninstalling 151
  bulk installing agents 122
  disabling rollback 142
Windows logon scripts
  response files 129