IBM Tivoli Asset Discovery for Distributed
Version 7.5

Configuring IBM Tivoli Asset Discovery for Distributed 7.5

IBM
IBM Tivoli Asset Discovery for Distributed
Version 7.5

Configuring IBM Tivoli Asset Discovery for Distributed 7.5
Configuration Guide

This edition applies to Version 7.5 fix pack 1 of IBM Tivoli Asset Discovery for Distributed 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.
Configuring Tivoli Asset Discovery for Distributed

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

Read the Configuring the server after installation - main steps section to find out which configuration steps are required and optional (after installing the administration server).
## Contents

Configuring Tivoli Asset Discovery for Distributed ........................ iii

Chapter 1. Configuring the server after installation: main steps ........ 1
Configuring permissions for users ........................................ 2
Configuring IBM Tivoli Asset Discovery for Distributed to work with IBM Tivoli Software
  Knowledge Base Toolkit ................................................. 3
    Step 1: Defining the URL for Software Knowledge Base Toolkit ........ 3
    Step 2: Enabling secure communication with Software Knowledge Base Toolkit ................................................. 4
  Importing new catalogs ................................................. 4
  Importing the processor value units table ................................ 5
  Importing a systems tier table ........................................ 6
  Importing part numbers .............................................. 6
  Configuring event notifications ...................................... 8
  Adding VM managers .................................................. 8
Configuring Tivoli Common Reporting to work with Tivoli Asset Discovery for Distributed ................................. 9
  Step 1: Preparing the database client for the administration server database (distributed scenario only) .................. 10
  Step 2: Connecting Tivoli Common Reporting with the administration server database (TLMA) .......................... 10
  Step 3: Importing the data model .................................... 11

Chapter 2. Configuring the administration server and agents .......... 13
Configuring the administration server .................................. 13
  Administration server settings ..................................... 13
  The log.properties file ............................................. 17
  Configuring the transaction log size ................................ 18
  Registering the administration server as a service ............... 18
Configuring agents ..................................................... 19
  Configuring agent parameters ...................................... 19
  Summary of agent configuration commands ......................... 21
  Agent settings ....................................................... 21
  Setting processor consumption limits on agents ................... 25
  Enabling the agent self-update ..................................... 26
  Configuring a scheduled agent self-update ......................... 29
  Configuring a periodic agent self-update .......................... 29
  Implementing and removing a test configuration .................... 30
  Configuring SELinux to work with the agent ........................ 30

Appendix ........................................................................ 33
Starting the server ....................................................... 33
Stopping the server ...................................................... 33

Notices ........................................................................ 35
Trademarks ...................................................................... 36

Index ............................................................................ 37

© Copyright IBM Corp. 2002, 2012
Chapter 1. Configuring the server after installation: main steps

There are eight configuration steps (required and optional) to perform after installing the server.

About this task

Perform postinstallation configurations:

1. Configure user permissions (optional)
   You can configure access rights for the users by assigning user to roles, for example Inventory administrator.

2. Configure secure connection with Software Knowledge Base Toolkit (optional only if you have installed the product on base WebSphere® Application Server)
   Configure secure connection between Tivoli Asset Discovery for Distributed and Software Knowledge Base Toolkit to enable automatic catalog distribution between the two products.

3. Import the most up-to-date software catalog (required)
   The catalog is a knowledge base that provides information required to recognize which products are installed and in use on monitored computers. Make sure that the catalog is in a canonical format.

4. Import the most up-to-date processor value unit table (required)
   The processor value unit table is required to support processor-based pricing models in which charges differ according to the type of processor on which the licensed product is installed and running.

5. Import the most up-to-date systems tier table (required)
   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.

6. Import the most up-to-date part numbers list (optional)
   Import a file with part numbers of the products that you have ordered. This will make it easier to resolve potential discrepancies in the right component bundling.

7. Configure event notifications (optional)
   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.

8. Configure VM managers (required if your infrastructure contains virtual machines)
   Add virtual machine managers to gather information about your VM infrastructure. This step applies only if you use supported virtualization technologies.

9. Configure Tivoli Common Reporting to work with the administration server (optional)
   Configure Tivoli Common Reporting to work with the administration server in order to be able to generate more accurate and detailed summary and trend reports.

Note: To ensure that the DB2® database works properly, you need to regularly back up your data and perform maintenance actions.
Configuring permissions for users

Create new users and grant them certain permissions by assigning them predefined roles, for example Administrator or softwareassetmanager.

Before you begin

You must have the role of iscadmins to perform this task.

About this task

A role is a set of permissions that provide a user with the ability to perform a predefined set of functions. A permission is a setting that specifies the system function or user interface element a user can access. Roles are typically defined to include related permissions, and usually correspond to a real-world role. You can assign multiple roles to a user, which grants the user the union of the permissions that define those roles.

Attention: In order to be able to add new roles to existing application users you must have the role iscadmins.

<table>
<thead>
<tr>
<th>Role</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>iscadmins</td>
<td>A role that can grant levels of authority to users.</td>
</tr>
<tr>
<td>administrator</td>
<td>A role that is responsible for Content Management.</td>
</tr>
<tr>
<td>inventoryadministrator</td>
<td>A role that can create and manage the monitoring infrastructure of servers, agents, nodes, and application users.</td>
</tr>
<tr>
<td>softwareassetmanager</td>
<td>A role that identifies, collects, maintains, and reports inventory of software assets throughout their life cycle.</td>
</tr>
</tbody>
</table>

Procedure

1. Log on to the Tivoli Integrated Portal user interface with the following default credentials:
   Hint:
   Tip: If this is the first login, you may use the credentials provided during the product installation.
The default values were:
   tipadmin
     administrator user ID
   typass
     administrator password

   Note: It is advisable to change these credentials after the first logging to Tivoli Integrated Portal user interface.

2. Create a user by performing the following steps:
   a. Expand the Users and Groups section of the navigation tree and click Manage Users. The WIM User Management panel opens.
b. Click **Create**. A new panel opens.
c. Complete all required fields and click **Create**.
d. On the confirmation panel click **Close**.

3. Assign the user to a chosen group:
   a. Expand the **Users and Groups** section of the navigation tree and click **User Roles**. A new panel opens.
   b. In the **User ID** field, provide the ID of the newly created user and click **Search**.
   c. In the search results section, click the new user ID. A new panel with **Available Roles** opens.
   d. Select the role you want to assign to the user, for example **inventoryadministrator**, and click **Save**.

**What to do next**

Now you may log out and log in as a newly created user or keep configuring permissions for more users.

**Tip:** You may consider removing the default administrator `tipadmin` if you have already finished the whole configuration process.

---

**Configuring IBM Tivoli Asset Discovery for Distributed to work with IBM Tivoli Software Knowledge Base Toolkit**

Define the URL for Software Knowledge Base Toolkit in the Tivoli Asset Discovery for Distributed web user interface. Next, Retrieve a signer certificate from a remote IBM Tivoli Software Knowledge Base Toolkit SSL port in order to enable automatic catalog distribution between both servers. Tivoli Asset Discovery for Distributed connects to the Tivoli Software Knowledge Base Toolkit remote SSL port and receives the signer information during the handshake using a trust manager.

**Before you begin**

- You must be an administrator to perform this task.

**Step 1: Defining the URL for Software Knowledge Base Toolkit**

**Before you begin**

Tivoli Asset Discovery for Distributed and Software Knowledge Base Toolkit must already be installed and running in your infrastructure.

**Procedure**

1. Log in to the Tivoli Asset Discovery for Distributed web user interface.
2. In the Tivoli Integrated Portal left navigation bar click **Import Software catalog**.
3. In the lower part of Manual Import section provide the host name or IP address of Software Knowledge Base Toolkit server and click **Apply**. Example: `https://localhost:12344`. You might also provide IP address.

**Results**

You have defined the location of Software Knowledge Base Toolkit server.
Step 2: Enabling secure communication with Software Knowledge Base Toolkit

Before you begin

The keystore that contains a personal certificate must already exist on the Software Knowledge Base Toolkit server and the connection to the server must be configured.

Procedure

1. Log in to the Tivoli Asset Discovery for Distributed web user interface.
2. In the Tivoli Integrated Portal left navigation bar, click Settings > WebSphere Administrative Console and then click the Launch WebSphere administrative console button.
3. In the WebSphere administrative console, click Security > SSL certificate and key management.
4. In the SSL certificate and key management panel, click on the Key stores and certificates link. In the table that opens, click NodeDefaultTrustStore.
5. On the NodeDefaultTrustStore pane, click the Signer certificates hyperlink, which is located in the upper right area of the pane. On the Signer certificates pane, click Retrieve from port button in the table header.
6. Provide the connection information in order to receive the Tivoli Software Knowledge Base Toolkit certificate. Provide the IP address of the Tivoli Software Knowledge Base Toolkit and the port number that will be used during the handshake. In the drop-down leave unchanged NodeDefaultSSLSettings and, in the next text field provide the Tivoli Software Knowledge Base Toolkit alias, for example swkbt_server.

Tip:

The alias specifies the certificate alias name that you want to use to reference the signer in the key store, which is specified in the SSL configuration.

For more details about the parameters that you need to provide see the Retrieve from port topic in the WebSphere Application Server information center.

7. Click the Retrieve signer information button. The certificate data appears. Click Apply and Save.
8. Restart the Tivoli Asset Discovery for Distributed server into which you have imported the signer certificate.

Results

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

Importing new catalogs

Import the software catalog after installation to keep your software inventory up-to-date.
Procedure

1. In the navigation bar, click Administration > Import Software Catalog.
2. You can import or upload the catalog.
   - In the Automatic Import section, click Import to automatically download and import the newer version (if it exists) of the catalog from Tivoli Software Knowledge Base Toolkit to the server. Before importing, you have to first publish the catalog in the knowledge base.
   - You can only import the catalog when the Software Knowledge Base Toolkit application is installed in your infrastructure and its Web address is specified in the Configure the Connection with Software Knowledge Base Toolkit expandable section in the Administration > Import Software Catalog window. You can also configure the URL by using the setserverconf command. First, you need to log in to the command-line interface. Then input the setserverconf -k SwKBToolURL -v SWKBT_URL command, where the SWKBT_URL parameter is the Web address of the application in the following format: protocol_name://hostname:port/ (for example, setserverconf -k SwKBToolURL -v https://9.156.44.150:12344/), and restart the server.
   - (Optional) If you have upgraded from Tivoli License Compliance Manager to Asset Discovery for Distributed on base WebSphere Application Server, you have to enable secure communication with Software Knowledge Base Toolkit.

The Importing Software Catalog window opens. In this window, you can view the status of import process.

Tip: The status is refreshed by default every 10 seconds. However, you can change the default value in Settings > Manage Global Refresh, or you can manually refresh the progress bar by clicking , and choosing Manual Refresh.

- Manually import the catalog from the knowledge base by clicking the Software Knowledge Base Toolkit link. To upload the catalog from your computer, in the Manual Import section, click Browse, select the file (in XML or ZIP format), and click Upload.

Attention: You cannot upload the catalog downloaded from the IBM website into Asset Discovery for Distributed. You have to import it using the knowledge base. Moreover, you can only use the catalog in a canonical format. You can find the catalog in such a format in the Canonical Form folder located in the Published Knowledge Base Content pane.

---

Importing the processor value units table

About this task

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

Note: The processor value unit table is updated periodically. Go to the IBM Tivoli Asset Discovery for Distributed support Web page, click Downloads and search for "PVU table" to download the latest version.
**Procedure**

1. In the navigation bar, click **Administration > Import PVU Table.**
2. You can perform two actions:
   - To automatically import the file from the IBM website, click **Import.**
   - To upload a PVU table from your computer, click **Browse**, select the file, and click **Upload.**

   **Tip:** If you want to download the XML files of the PVU tables, go to the following FTP address:

---

**Importing a 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.

**About this task**

The systems tier table is required to support the tier-based pricing model in which charges differ according to the level in which given servers fall. There are three levels or tiers: small, medium, and large. They denote a value that is assigned to a product and to a server on which it is installed. The table contains combinations of system models and products that are queried to find the tiers with which they are associated.

**Note:** The tier table is updated periodically. Go to the [IBM Tivoli Asset Discovery for Distributed support](https://www.ibm.com/support/pages/node/554689) Web page and search for "tier table" to download the latest version.

**Procedure**

1. In the navigation bar, click **Administration > Import Systems Tier Table.**
2. You can perform two actions:
   - To automatically import the file from the IBM website, click **Import.**
   - To upload the tier table from your computer, click **Browse**, select the file, and click **Upload.**

---

**Importing part numbers**

You can import a file with part numbers of the products that you have ordered.

This action makes it easier to resolve potential discrepancies in the right component bundling.

**About this task**

Importing part numbers is a feature that lets you upload to the server the list of part numbers that are related to the products in your infrastructure. The part numbers are helpful when it comes to resolving any difficulties during component bundling. After you upload the file, the confidence level of the products with part numbers increases.

**Procedure**

1. Create a part numbers list. You have two options:
• You can download the file with your part numbers directly from Passport Advantage®:
  a. Log in to Passport Advantage.
  b. From the menu on the left, select Reporting > Order history.
  c. If applicable, select the relevant site or sites.
  d. In the Type of order section, select All.
  e. Specify the Sales order date.
  f. Select any option from the Sort by list, and click Submit detail report.
  g. Your report is ready. Click Download report to save it, and then select Comma delimited.
• You can create such a file on your own:
  – You can use a text editor. In this case, enter each part number in a new line.
  – You can use a CSV file with multiple columns. The column with part numbers must be called Part number. Use a comma as a field separator and quotation marks (" ") as a text delimiter. For example:
    "Part number","Order type"
    "D07UMLL","Licenses"
    "D08UMLL","Licenses"
    "D09UMLL","Licenses"

  Tip: Only the column named Part number is treated as the one that contains part numbers. If you name any other column Order type, only the rows that contain the "Licenses" element are imported.

In most cases, only part numbers that refer to license purchases should be used for automated bundling. However, it might happen that your order history does not contain initial license purchases for some products but only subsequent subscription or support part numbers. It is possible to use these part numbers for automated bundling. Create a CSV file with a single column in which you list each part number in a new line. For example:
  D07UMLL
  D08UMLL
  D09UMLL
All part numbers from this file will be used during automated bundling.

2. In the navigation bar, click Administration > Import Part Numbers.
3. Only if service providers functionality is enabled: From the drop-down list, select the report group to which you want to import the part numbers.
4. Optional: Select the check box at the bottom of the page to delete the previous part numbers list form the server. If you delete it, instances that are bundled with products based on the part numbers information will not be bundled any more.
5. Upload the file from your computer by clicking Browse, selecting the file, and clicking Upload.

  Tip: You can also upload the packed files in the .zip or .gzip format.
What to do next

You can see the results of your actions in the Part Numbers column in the Manage Software Inventory panel. If there are no components assigned to products, it means that the product has not been installed yet or it has not been discovered by the software scan yet.

**Remember:** When you buy a new part number, import it to the server. Even if there are any duplicate part numbers, only one entry is taken into account. All part numbers that are imported by you are marked in the reports with the ☑ icon.

Configuring event notifications

You can configure the server to generate email notifications of significant licensing and system administration events. The notifications are then sent to recipients that you select in the Web interface.

**Procedure**

1. To set the SMTP server, run the setserverconf command with the parameters: `setserverconf -k smtpServer -v ip_address`, where
   
   `ip_address`
   
   The IP address of your SMTP server.

2. To set the mail sender, run the setserverconf command with the parameters: `setserverconf -k mailSender -v email_address`, where

   `email_address`
   
   The email address from which the notifications are sent.

   For a complete description of the parameters, see “Administration server settings” on page 13.

3. Restart the server.

4. Log on to the Tivoli Integrated Portal as an administrator.

5. In the navigator pane, select Tivoli Asset Discovery for Distributed > Administration > Manage Notifications.

6. Select Add Subscriber from the dropdown list.

7. In the Add Notification Subscriber page, specify the recipient of notification e-mails, and the events to which they are assigned.

8. Click OK to save and close, or Save and Add Another to add another recipient.

Adding VM managers

You have the option of adding virtual machine managers to gather information about your VM infrastructure.

**Before you begin**

- You must be an inventory administrator to perform this task.

**Procedure**

1. In the navigation bar, click Infrastructure > VM Managers.

2. From the Select Action list, choose Add VM Manager.
**Tip:** Make sure that the user ID has read access to virtual machines and hosts (and potentially to clusters) that host these VMs. Write access is not required. You can verify the access rights by checking whether in VMware Infrastructure Client the user ID has correct access privileges for all the components in the hierarchy.

3. Specify the full URL, host name, or IP address of the VM manager. If you specify the host name or IP address, the full VM manager address is built on the server side based on the selected type of the VM manager. If you provide the full web address, you must specify the protocol, for example: https://virtualcenter/sdk. Refer to the VM manager documentation in case of any problems. Note also that each configured VM manager must have different web address, that is, only one entry is allowed for a particular URL.

4. Select the type of the VM manager.

5. **Optional:** If you chose Microsoft Hyper-V, select one of the available communication interfaces: PowerShell or NTLM.

6. **Optional:** If you chose Microsoft Hyper-V, you can share credentials with other hosts in the same cluster. To do so, select the **Share credentials with other hosts in the same cluster** check box.

7. Specify the user name and password for connecting with the VM manager.

   **Note:** Different definitions of users are used for Microsoft Hyper-V and VMware:
   - For Microsoft Hyper-V, you must use the Administrator account. The user name must contain the domain name and be defined as `domain\username` or `username@domain`. For example: `cluster.com\Administrator` or `Administrator@cluster.com`. If the target server is not in a domain, specify its host name as the domain. For example: `hostname\Administrator` or `Administrator@hostname`.
   - For VMware, the user is defined as `domain\username`. For example: `cluster.com\test`.

8. To test the connection, click **Test connection**.

9. If you successfully connected to the specified VM manager, click **OK** to save its parameters. You can save the settings and add another VM manager by clicking **Save and Add Another**.

   **Note:** You can use the `setserverconf -k vmManagerPollingInterval -v value` command to change the settings of the polling interval. By default, the time between two communication attempts with a particular VM manager is 30 minutes. The minimum value is 30 and the maximum is 10080 minutes (seven days). Restart the server for the changes to take effect.

---

**Configuring Tivoli Common Reporting to work with Tivoli Asset Discovery for Distributed**

Configure Tivoli Common Reporting to work with Tivoli Asset Discovery for Distributed in order to be able to generate more accurate and detailed summary and trend reports.
Step 1: Preparing the database client for the administration server database (distributed scenario only)

Before you begin

This task is to be performed if the administration server database is on a computer other than the one where Tivoli Common Reporting is installed.

Procedure

1. Perform the installation of DB2 client on the computer where Tivoli Common Reporting is installed. For installation information see [DB2 information center](#).
2. Restart Tivoli Common Reporting after the installation of DB2 client.
3. Start the profile: `su profile_name`.
4. Start DB2, issue `DB2` and press `Enter`.
5. Issue the following commands to perform the cataloging of the administration server database (TLMA):
   ```
   CATALOG TCPIP NODE DB_node_name REMOTE DB_server_IP_address SERVER port_number
   CATALOG DB TLMA AS database_alias AT NODE DB_node_name
   ```
   where
   - **DB_node_name**
     Represents a nickname you can set for the computer that contains the database you want to catalog.
   - **DB_server_IP_address**
     The IP address of the node where the administration server (TLMA) database resides.
   - **port_number**
     Specifies the port number of the server database manager instance.

   **Note:** You must use TLMA database name; otherwise you will not be able to connect Tivoli Common Reporting with the TLMA database.

   Example:
   ```
   CATALOG TCPIP NODE node_kb REMOTE 9.156.44.150 SERVER 50000
   CATALOG DB TLMA AS TLMA AT NODE node_kb
   ```

Step 2: Connecting Tivoli Common Reporting with the administration server database (TLMA)

Before you begin

- Tivoli Asset Discovery for Distributed and Cognos-based Tivoli Common Reporting must already be installed and running in your infrastructure.
- A DB2 database client must be installed on the computer where the Tivoli Common Reporting engine is installed.

Procedure

1. Logon to the Tivoli Common Reporting web user interface at the following URL: `http://host_name:16310/ibm-console`

   **Note:** If you installed Tivoli Asset Discovery for Distributed before Tivoli Common Reporting, the port number is different.

2. In the left navigation bar click **Reporting > Common Reporting**. In the drop-down list located in the upper right corner click **Launch >**
Administration.

A new pane opens.

3. To add new data source click the **Configuration** tab and then the ![icon] icon.

4. On the **New Data Source wizard**, provide the following information:
   - a. On the first pane of the wizard, provide the name of the database: TLMA. Click **Next**.
   - b. Specify the type of the database: DB2. Leave **Use the default object gateway** selected and click **Next**.
   - c. On the third pane, specify TLMA as the name of the DB2 database and leave the **Signons** radio button selected. Select the **Password** checkbox and leave **Create a signon that the Everyone group can use** selected. Provide the user ID (tlmsrv) and the password for the TLMA database. To verify the connection with the TLMA database click **Test the connection...** link and then the **Test** button. A new pane opens informing that the connection was successful. Click **Close**, and then, on the following pane click **Close** again. Click **Next** to proceed to the last pane.
   - d. Click **Finish** to exit the wizard.

**Results**

You have successfully connected Tivoli Common Reporting with the administration server database.

**Step 3: Importing the data model**

**Procedure**

1. Copy the TAD4D-reports-7.5.0.zip into the following directory:
   - **UNIX**: /opt/IBM/tivoli/tipv2Components/TCRComponent/cognos/deployment
   - **Windows**: C:\IBM\tivoli\tipv2Components\TCRComponent\cognos\deployment

   You can download the file from Passport Advantage or from the product DVD.

2. Log on to the Tivoli Common Reporting interface.

3. In the left navigation bar click **Reporting > Common Reporting > Launch** and then **Administration**.

4. On the Configuration tab click **Content Administration**. A new page opens.
5. Create a package import by clicking the icon located in the upper right side of the page. A new wizard opens.

6. On the new page, select the radio button with the name of the package you copied in step 1 and click **Next**.

7. A wizard starts.
   a. On the first page, in the name field, provide the name of the reports and click **Next**.
   b. On the next page, in the **Public folders content** section, select the reports you defined in the previous step and click **Next**.
   c. On the **Specify the general options - New Import wizard** page click **Next**.
   d. On the **Review the summary - New Import wizard** page read the information and click **Next**.
   e. On the final page select **Save and run once** and click **Finish**.

8. The **Run with options - TAD4D reports** page opens. Select **Now**, leave **Keep the existing report specification versions** selected, and click **Run**.

9. On the new **IBM Cognos 8** page select **View the details of this import after closing this dialog** (optional) and click **OK**.

10. Restart Tivoli Common Reporting.

**Results**

You have imported Tivoli Asset Discovery for Distributed data model into Tivoli Common Reporting.
Chapter 2. Configuring the administration server and agents

You can perform additional configurations in IBM Tivoli Asset Discovery for Distributed as you continue using the product.

Configuring the administration server

You can perform additional configurations in IBM Tivoli Asset Discovery for Distributed to tune the server or improve its performance.

Administration server settings

Read about the configuration settings for the Tivoli Asset Discovery for Distributed server and how you can modify some of them to tune the product to suit your needs. This table shows the server parameters defined in the server database.

To set the value of a server configuration parameter, enter the following command into the command-line interface:

```
setserverconf -k parameterName -v parameterValue
```

Note: The changes take effect after you restart the server. You can check if you have set the correct parameter value by issuing the `getserverconf -k parameterName` command. However, you will not be able to validate the format of certain values entered, as some formats can be treated as strings (for example minutes or percents).

The timing of events, in particular of services on the administration server is determined by two factors: the start time and the period between events. Each event has a parameter that determines its frequency. The start time is determined by the time that the server last started. The only exception to this rule is the `aggregateUsageTime` parameter.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Units</th>
<th>Default</th>
<th>Minimum</th>
<th>Maximum</th>
</tr>
</thead>
<tbody>
<tr>
<td>agentCacheRefreshInterval</td>
<td>minutes</td>
<td>60</td>
<td>5</td>
<td>2880</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>The interval at which the cache that contains parameters downloaded by the agent is refreshed.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>agentInitializationTime</td>
<td>seconds</td>
<td>60</td>
<td>0</td>
<td>3600</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>96400</td>
</tr>
</tbody>
</table>

Determines the length of the period between the first plugin (to the administration server) and hardware scan that agents are to perform.
### Table 2. Server configuration parameters in the database.  (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Units</th>
<th>Default</th>
<th>Minimum</th>
<th>Maximum</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>agentToServerSecurityLevel</strong></td>
<td>0, 1, 2</td>
<td>0</td>
<td>0</td>
<td>2</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Determines the level of security to be used for communications between agents and the <em>msghandler</em> server. Possible values are:</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>0</td>
<td>Communication is through the nonsecure port.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>1</td>
<td>Communication is through the secure port with server authentication.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>2</td>
<td>Communication is through the secure port with server and client authentication.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> Agents with medium security levels can communicate with <em>msghandler</em> server that has security levels of minimum (0) or medium (1), provided that both the secure and nonsecure ports are configured. If the maximum security level is used, both the agent and its <em>msghandler</em> server must be aligned with the security level set to maximum.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>agentVmManagerDetachmentPeriod</strong></td>
<td>minutes</td>
<td>1440</td>
<td>180</td>
<td>10800 (7.5 days)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>The maximum idle time before an agent managed by a VM manager is considered detached. From that point in time, the data sent by an agent will not be augmented by the data retrieved from the VM manager.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>aggregateUsageTime</strong></td>
<td>hour of day</td>
<td>00:00</td>
<td>00:00</td>
<td>23:59</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>The daily start time for aggregations of the data in the inventory tables (in the local time). The aggregation process aggregates qualifying inventory information (see <strong>maxAggregateUsageAge</strong> below) by product and server, and stores it in the corresponding history tables.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Each aggregation is logged in the server trace file.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>catalogBuilderPeriod</strong></td>
<td>minutes</td>
<td>1440</td>
<td>180</td>
<td>10080 (1 week)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>The interval between consecutive builds of the catalog. After each build, agents download the new catalog.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>csvReportRowCount</strong></td>
<td>integer</td>
<td>2147483647</td>
<td>1</td>
<td>9223372036854775807</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Controls the number of records that are read from the database in one read operation, that are to be saved to a CSV report file. If the report to be saved to the CSV file is very large, the read operation may cause high memory usage on the server. To resolve this problem, decrease the <strong>csvReportRowCount</strong> value to a lower value. This will reduce the memory used in the operation, but may also increase the time to generate the report file.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>csvReportSeparator</strong></td>
<td>character</td>
<td>comma</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>The type of separator that is used in the csv file, for example, a comma or hyphen (only one character is accepted).</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>discoveryMinConfidenceLevel</strong></td>
<td>percents</td>
<td>90</td>
<td>0</td>
<td>100</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Describes the minimum confidence level for the imported network discovery results (for example from nmap) to be saved in the database.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>divisionPluginLevel</strong></td>
<td>0, 1, 2</td>
<td>1</td>
<td>0</td>
<td>2</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Defines how the agent connects to the default scan group for the first time. The possible settings are:</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>0</td>
<td>The agent never connects to the default scan group.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>1</td>
<td>The server tries to connect the agent to the scan group that has been defined for it. If the group does not exist, the server connects the agent to the default group.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>2</td>
<td>The agent always connects to the default scan group; the server ignores the scan group the agent has sent even if it exists.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Table 2. Server configuration parameters in the database. (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Units</th>
<th>Default</th>
<th>Minimum</th>
<th>Maximum</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>fipsEnabled</strong></td>
<td></td>
<td>true/false</td>
<td>false</td>
<td></td>
</tr>
<tr>
<td>Determines whether FIPS 140-2 certificated modules are to be used to transmit encrypted data. Possible values are:</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>false</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Encrypted data is transmitted using default modules.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>true</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Encrypted information is transmitted using FIPS 140-2 certificated modules.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

| inactivateDuplicatedAgentEnabled  | true/false | false |          |          |
| Determines whether the Unknown status is activated. |
| true | | | | |
| If duplicated agents were installed on the same physical host in sequence, the last installed agent remains active. The agents that plugged into the server earlier are indicated with the status Unknown. |
| **Tip:** For more information about agent statuses, see *Agent statuses*. |
| false | | | | |
| If you add another duplicated agent, it is displayed as Active. |
| **Note:** Setting the *inactivateDuplicatedAgentEnabled* property to false will not result in deactivation of the Unknown status of the duplicated agent that was detected before the value was changed. |

| inactivateDuplicatedAgentPeriod   | minutes | 1440 | 1440 | 129600 |
| The interval between the updates to the Unknown status. |

| includeSharedProductsInCalculations | true/false | false |          |          |
| This is used for PVU and STG calculations. The permitted values are: |
| true | | | | |
| The product instances that are discovered on a shared file system are included in an audit report regardless of whether the software usage of those products was detected or not. |
| false | | | | |
| The product instances that are discovered on a shared file system are included in an audit report only if usage of those products was detected. |

| inventoryScanAllowedClockSkew     | hours | 1 | 0 | 6 |
| The amount of time that the agent can start the scan before the specified time. It is used to identify the inventory scan which had started a little before the scheduled start. If it is turned on "1", it will allow to treat the scan from, for example, Friday 5.55 p.m. as the scan from Friday 6.00 p.m. and not Thursday 6.00 p.m. (if scans are done every day). |

| inventoryScanAllowedClockSkewTLCM23Agent | hours | 10 | 1 | 24 |
| The amount of time that Tivoli License Compliance Manager 2.3 agents can start a scan before the specified time. The exact scan time in the agent local time is unknown. For agents that are in a time zone earlier than the server, the scans arrive at the server before the scheduled start time. The *inventoryScanAllowedClockSkewTLCM23Agent* enables these early scans to be accepted. For example, if the scan arrives at the server 10 hours before the scheduled time and the *inventoryScanAllowedClockSkewTLCM23Agent* parameter value is 10, the agent scan status will be OK. The value of the parameter should be adjusted to the biggest time zone difference between the server and the agent in your infrastructure. |

| inventoryScanGracePeriod         | hours | 10 | 1 | 336 (2 weeks) |
| The period during which agents are to send inventory data back to the server. After that, the software scan is marked as failed. |

| mailSender                       | email address |          |          |          |
| The email address that is used by the server as the sender address when notifications are generated. The text must include only US ASCII characters. |

| maxAgentInactivity               | minutes | 1440 (1 day) | 1440 (1 day) | 129600 (3 months) |
| The maximum time that an agent does not communicate before it is considered as not connecting. |
Table 2. Server configuration parameters in the database. (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Units</th>
<th>Default</th>
<th>Minimum</th>
<th>Maximum</th>
</tr>
</thead>
<tbody>
<tr>
<td>maxAgentInactivityToDelete</td>
<td>minutes</td>
<td>43200 (30 days)</td>
<td>20160 (2 weeks)</td>
<td>518400</td>
</tr>
<tr>
<td>The maximum time after which an agent which is considered inactive will be removed from the system.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>maxAggregateUsageAge</td>
<td>days</td>
<td>2</td>
<td>2</td>
<td>14</td>
</tr>
<tr>
<td>The age of the use data (in days) before it is included in the aggregations of the unaggregated software use database tables. This setting is used to ensure that all the relevant data for an aggregation has arrived at the server, taking into account the frequency with which it is uploaded from the agent. <strong>Important</strong>: To ensure that all the relevant use data is aggregated, you can set the value of the parameter to be greater than the value of the <code>upload_usage_period</code> parameter.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>maxPdfRows</td>
<td>number of rows</td>
<td>8000</td>
<td>1</td>
<td>16000</td>
</tr>
<tr>
<td>The maximum number of rows that can show up on a PDF file retrieved from the UI. This number is twice the number of maximum products instances that can show up in an audit report PDF. For example, if <code>maxPdfRows</code> is specified to be 8000, up to 4000 instances can show up in the report.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Fix Pack 1 maxRESTRowsRead</td>
<td>number of instances</td>
<td>1000</td>
<td>1</td>
<td>20000</td>
</tr>
<tr>
<td>The maximum number of software instances that can be retrieved in a single request.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Fix Pack 1 maxRESTRowsWrite</td>
<td>number of instances</td>
<td>1000</td>
<td>1</td>
<td>10000</td>
</tr>
<tr>
<td>The maximum number of software instances that can be updated in a single request.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>maxSubsequentCredentialFailures</td>
<td>number of tries</td>
<td>3</td>
<td>0</td>
<td>100</td>
</tr>
<tr>
<td>The maximum number of failed attempts to log in to the VM manager. After the set number of failed connection attempts, the account is locked. The value 0 indicates unlimited attempts.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>nodeTag</td>
<td>string</td>
<td>%VENDOR %TYPE %NAME</td>
<td></td>
<td></td>
</tr>
<tr>
<td>The structure used when the Tivoli Asset Discovery for Distributed server assigns node tags during the automatic creation of node records. These values are displayed in the Web user interface and you can determine if all of them are to be displayed.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>productInventoryBuilderPeriod</td>
<td>minutes</td>
<td>300</td>
<td>300</td>
<td>4320 (3 days)</td>
</tr>
<tr>
<td>The interval between consecutive builds of the inventory on the server. At this interval of time, the server reconciles the installed software information collected by the agent, which identifies the software components that are installed on monitored computers, with the product information held on the server. In this way the inventory of components is converted to an inventory of products, in which components are assigned according to the catalog information and the mappings of shared components.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>recalculationPeriod</td>
<td>minutes</td>
<td>10</td>
<td>5</td>
<td>1440</td>
</tr>
<tr>
<td>Determines the length of the period between two consecutive recalculations.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>reportPath</td>
<td>full path</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>The path to the directory where the report will be generated prior to signing. If there is not enough space in the default directory, the generating of the report fails (it includes report signing and exporting to xml).</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Parameter</td>
<td>Units</td>
<td>Default</td>
<td>Minimum</td>
<td>Maximum</td>
</tr>
<tr>
<td>---------------------------------------</td>
<td>-------</td>
<td>---------</td>
<td>---------</td>
<td>---------</td>
</tr>
<tr>
<td>smtpServer</td>
<td>hostname or IP address</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Description</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>softwareScanStatusCalculation</td>
<td>minutes</td>
<td>720</td>
<td>60</td>
<td>2880</td>
</tr>
<tr>
<td>Period</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Description</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>storeHwDataForAllVMManagerNodes</td>
<td>true/false</td>
<td>false</td>
<td>true</td>
<td>false</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Description</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>storeUser</td>
<td>true/false</td>
<td>true</td>
<td>true</td>
<td>false</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Description</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SwKBToolURL</td>
<td>text</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Description</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>testEnvironmentEnabled</td>
<td>true/false</td>
<td>false</td>
<td>true</td>
<td>false</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Description</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>vmManagerConnectionTimeout</td>
<td>milliseconds</td>
<td>90000</td>
<td>1</td>
<td>2147483647</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Description</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>vmManagerPollingInterval</td>
<td>minutes</td>
<td>30</td>
<td>30</td>
<td>10080</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Description</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>vmManagerPostprocessGuestEnabled</td>
<td>true/false</td>
<td>true</td>
<td>true</td>
<td>false</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Description</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>websiteWithCatalogs</td>
<td>URL</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Description</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>websiteWithPVUs</td>
<td>URL</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Description</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**The log.properties file**

The log.properties file defines the trace parameters for the IBM Tivoli Asset Discovery for Distributed server.

Chapter 2. Configuring the administration server and agents 17
The trace parameters (\texttt{itm.trace logger.level}, \texttt{itm.trace file handler.max file bytes}, \texttt{itm.message file handler.max files}, \texttt{itm.trace file handler.max files} and \texttt{itm.message file handler.max file bytes}) are the only parameters in the log.properties file that can be changed and reloaded while the server is running. See the Troubleshooting and support section of the information center for full details. After you have modified the settings, use the \texttt{logreload} command to reload them.

There are two log.properties files, located in the following directories:

<table>
<thead>
<tr>
<th>Platform</th>
<th>File location</th>
</tr>
</thead>
<tbody>
<tr>
<td>UNIX</td>
<td>$\text{was_install_dir}/profiles/TIPProfile/installedApps/TIPCell/isc.ear/tad4d_admin.war/WEB-INF/conf/log.properties</td>
</tr>
<tr>
<td>Linux</td>
<td>$\text{was_install_dir}/profiles/TIPProfile/installedApps/TIPCell/LMT-TAD4D_Agent_message_handler.ear/com.ibm.license.mgmt.msghandler.web.war/WEB-INF/conf/log.properties</td>
</tr>
<tr>
<td>Windows</td>
<td>$\text{was_install_dir}/profiles\TIPProfile\installedApps\TIPCell\isc.ear\tad4d_admin.war\WEB-INF\conf\log.properties</td>
</tr>
<tr>
<td></td>
<td>$\text{was_install_dir}/profiles\TIPProfile\installedApps\TIPCell\LMT-TAD4D_Agent_message_handler.ear\com.ibm.license.mgmt.msghandler.web.war\WEB-INF\conf\log.properties</td>
</tr>
</tbody>
</table>

### Configuring the transaction log size

After Asset Discovery for Distributed is installed, set the size of the DB2 transaction log and the number of primary and secondary DB2 log files.

**About this task**

The size of the transaction log and the number of log files are set with DB2 configuration values. The transaction log size, and the number of log files that are required depends on the number of agents and discovered components in your infrastructure.

**Note:** To avoid problems with importing the catalog, increase the DB2 transaction log size and the number of log files before you import the catalog.

For small and medium-sized environments of up to 20000 agents, use the following values for the transaction log size and the number of log files.

- \texttt{LOGFILSIZ} = 20000
- \texttt{LOGPRIMARY} = 155
- \texttt{LOGSECOND} = 100

For environments with more than 20000 agents, specify the value of the \texttt{LOGFILSIZ} parameter that is up to two times bigger than the value for a small or medium-sized environment. The number of primary and secondary logs cannot exceed 255, so the values of the \texttt{LOGPRIMARY} and \texttt{LOGSECOND} parameters for larger environments are the same as above.

### Registering the administration server as a service

If the administration server is registered as a service, it will start automatically after the computer has rebooted.
About this task

Use a method of starting the service (Windows) or daemon (UNIX, Linux) specific to your operating system and its release. For example, on Linux systems, an administrator typically writes a startup script and places it in `/etc/init.d` directory. For more information how to create startup scripts, see the documentation of your operating system.

Configuring agents

This section describes the means to manage changes in the agent configuration using a set of commands to be issued from the Tivoli Asset Discovery for Distributed command line.

It provides the following capabilities:

- To set agent parameters at all agents level or scan group level.
  
  A parameter inherits a value from a different parameter unless it is specified in other way. For example, if you set a value for a parameter at all agents group level, all agents will use that value unless a different value has been set for a scan group of any agent.
  
  If you want the new value that you have applied at a higher level to apply to lower levels that have their own values set, you can choose to remove or suspend the values that are set at the lower levels. Values that have been suspended can later be reinstated.

- To schedule agent self-update to be performed in a specified timeslot.

- To suspend or activate defined values for agent parameters at all agents level or scan group level.

  The state of the defined parameter can be set to active or hold. By controlling the state of parameters you can prepare an agent configuration ahead of time, putting each parameter on hold until the time comes to activate the new configuration.

- To view details of the parameter values applied at all agents level or scan group level.

Configuration changes that you make using the commands are stored in the Tivoli Asset Discovery for Distributed server database and are then downloaded to agents. Take into account the time required for download services between the Tivoli Asset Discovery for Distributed server and agents when defining configuration changes, in particular date settings that are in the immediate future.

Configuring agent parameters

Each Tivoli Asset Discovery for Distributed agent parameter has a default state and value. You can use the `setagentconf` command to override defaults for all agents or for a scan group. For example, you can set the frequency of hardware and software scans.

Before you begin

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

- The command-line interface must be able to connect to the server using address "localhost".
• Security must be enabled on the server.

**About this task**

You can optionally set parameters to one of the following states:
• Active.
• Hold, which means that parameter is ignored.

In the following tables, the third column shows how the value of a particular agent parameter depends on whether you also set the *state* for that parameter, and whether you set the state for all agents or just one scan group.

<table>
<thead>
<tr>
<th>Level of override</th>
<th>Parameter state</th>
<th>Parameter value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scan group (-d &lt;groupname&gt;)</td>
<td>hold, or not set</td>
<td>The system default is used.</td>
</tr>
<tr>
<td>General (-a11)</td>
<td>hold, or not set</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Level of override</th>
<th>Parameter state</th>
<th>Parameter value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scan group (-d &lt;groupname&gt;)</td>
<td>hold, or not set</td>
<td>The general override is used.</td>
</tr>
<tr>
<td>General (-a11)</td>
<td>active</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Level of override</th>
<th>Parameter state</th>
<th>Parameter value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scan group (-d &lt;groupname&gt;)</td>
<td>active</td>
<td>The scan group override is used.</td>
</tr>
<tr>
<td>General (-a11)</td>
<td>active, hold, or not set</td>
<td></td>
</tr>
</tbody>
</table>

**Note:** You cannot modify the system default value.

**Procedure**

1. Access the command-line interface.
2. Log in to the server.

   **Note:** If you decide to perform this task in non-interactive mode, you will be required to log in with your username and password with each command you run.

3. At the command line, type the `setagentconf` command with the following options:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-a11</td>
<td>Sets the configuration key for all agents. You must specify either the -a11 or -d option.</td>
</tr>
<tr>
<td>-d scanGroup</td>
<td>The name of the scan group for which the configuration is being set. That is, the configuration is set for the whole scan group rather than particular agents. You must specify either the -a11 or -d option.</td>
</tr>
<tr>
<td>-k parameterName</td>
<td>Required. The name of the agent configuration parameter.</td>
</tr>
<tr>
<td>-v parameterValue</td>
<td>Optional. The value for the specified agent configuration parameter.</td>
</tr>
</tbody>
</table>
Option  |  Description
--- | ---
-s state{active | hold} | Optional. Specifies the state of the value of an agent configuration parameter. The mutually exclusive values are:
  • active
    Default. When the state of the parameter value is set to active, the value of the parameter is effectively used.
  • hold
    When the state of the value of a parameter is set to hold, the value of the parameter is kept in the server database and is not used.

-r | -h | Optional. Mutually exclusive parameters that make changes on the scan group level. When -r is used, configuration keys for the scan group level are removed. When -h is used, configuration keys on the scan group level are preserved and their states are set to "hold". In both cases the effective value is the one currently set. Relevant only when used with the -all parameter.

For a complete list of parameters that can be set using the setagentconf command, see [setagentconf command](#).

4. Press Enter.

**Example**

To set the value of the ping_period parameter to 300 for scan group abc, enter:

```bash
setagentconf -d abc -k ping_period -v 300
```

To set the value of the ping_period parameter to 400 and make its state hold for all agents that belong to scan group abc, enter:

```bash
setagentconf -d abc -k ping_period -v 400 -s hold
```

**Summary of agent configuration commands**

This topic contains the list of commands introduced for the agent configuration management feature.

*Table 4. Agent configuration commands*  
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>setagentconf</td>
<td>Sets the value and, optionally, the state of the agents configuration parameter.</td>
</tr>
<tr>
<td>getagentconf</td>
<td>Retrieves the values of configuration parameters for a specific agent.</td>
</tr>
<tr>
<td>delagentconf</td>
<td>Deletes the value of a configuration parameter for a specified agent.</td>
</tr>
</tbody>
</table>

**Agent settings**

This table shows the parameters defined in the server database.
Note: The agent parameters that you can manage by using the agent configuration management feature include the parameters that control the scheduling of software and hardware inventory scans. The principal means of scheduling software scanning is by using the web UI task. You can change the scan-related parameters by using the agent configuration management commands. For consistency with the scan scheduling methods, you cannot make changes at the individual agent level.

Use the setagentconf command to change the value of a parameter. For a detailed description of the syntax of this command, see the setagentconf command in the "Commands" section of the information center.

Table 5. Agent configuration parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Units</th>
<th>Default</th>
<th>Minimum</th>
<th>Maximum</th>
<th>Supported agents</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Fix Pack 1 cpu_threshold</strong></td>
<td>percents</td>
<td>100</td>
<td>5</td>
<td>100</td>
<td><strong>Description</strong> Defines the maximal CPU consumption of the agent during the software scan. For more information, see: Setting processor consumption limits on agents.</td>
</tr>
<tr>
<td><strong>Interim Fix 4</strong></td>
<td>start</td>
<td>Interim Fix 4</td>
<td></td>
<td></td>
<td>Starting from interim fix 4, the cpu_threshold parameter functionality is extended. In addition to limiting the CPU consumption of the software scan, it also limits the CPU consumption of the use scan and hardware scan. <strong>Note:</strong> If you reduce the value of this parameter, the time required to perform a software scan increases.</td>
</tr>
<tr>
<td>dependency_report_period</td>
<td>seconds</td>
<td>360</td>
<td>5</td>
<td>604800</td>
<td>Tivoli Asset Discovery for Distributed 7.5 fix pack 1 except for IBM i (formerly i5/OS™)</td>
</tr>
<tr>
<td>dependency_scan_count</td>
<td>integer</td>
<td>5</td>
<td>1</td>
<td>10000</td>
<td>Tivoli Asset Discovery for Distributed 7.5 fix pack 1 except for IBM i (formerly i5/OS)</td>
</tr>
<tr>
<td>dependency_scan_period</td>
<td>seconds</td>
<td>300</td>
<td>5</td>
<td>604800</td>
<td>Tivoli Asset Discovery for Distributed 7.5 fix pack 1 except for IBM i (formerly i5/OS)</td>
</tr>
</tbody>
</table>
### Table 5. Agent configuration parameters (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Units</th>
<th>Default</th>
<th>Minimum</th>
<th>Maximum</th>
<th>Supported agents</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>down_parms_period</strong></td>
<td>minutes</td>
<td>360</td>
<td>180</td>
<td>10080 (1 week)</td>
<td>All</td>
</tr>
<tr>
<td>Description</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>The interval between the downloads of the agent parameters from the server. In addition to the parameters, at each download, the agent checks the date of the last catalog update at the server. It also downloads the catalog if its own catalog is older.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>hw_inv_rate_type</strong></td>
<td>integer</td>
<td>3</td>
<td>0</td>
<td>3</td>
<td>All</td>
</tr>
<tr>
<td>Description</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Defines the unit in which the <strong>hw_inv_rate_value</strong> parameter is expressed. The <strong>hw_inv_rate_type</strong> together with <strong>hw_inv_rate_value</strong> define the repetition period of the hardware scan.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>The possible values are:</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>0</td>
<td>No repetition.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>1</td>
<td>1 day</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>2</td>
<td>7 days (a week)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>3</td>
<td>30 days (a month)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>For example, if <strong>inv_rate_type=3</strong> and <strong>inv_rate_value=5</strong>, the hardware scan repeats every 5 months.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>hw_inv_rate_value</strong></td>
<td>integer</td>
<td>1</td>
<td>1</td>
<td>9999</td>
<td>All</td>
</tr>
<tr>
<td>Description</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>The number of repeating periods, as defined by <strong>hw_inv_rate_type</strong>, that separate the consecutive occurrences of the hardware scan.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>hw_inv_start_date</strong></td>
<td>date</td>
<td></td>
<td></td>
<td></td>
<td>All</td>
</tr>
<tr>
<td>Description</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>The date and time when the first or only occurrence of the hardware inventory scan is performed. The format is YYYY-MM-DD.hh.mm.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>hw_scan_enabled</strong></td>
<td>Boolean</td>
<td>1</td>
<td>0</td>
<td></td>
<td>All</td>
</tr>
<tr>
<td>Description</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Enables hardware scan.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>0</td>
<td>Disabled.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>1</td>
<td>Enabled.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>inv_rate_type</strong></td>
<td>integer</td>
<td>2</td>
<td>0</td>
<td>3</td>
<td>All</td>
</tr>
<tr>
<td>Description</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Defines the unit in which the <strong>inv_rate_value</strong> parameter is expressed. The <strong>inv_rate_type</strong> together with <strong>inv_rate_value</strong> define the repetition period of the software scan.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>The possible values are:</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>0</td>
<td>No repetition.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>1</td>
<td>1 day</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>2</td>
<td>7 days (a week)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>3</td>
<td>30 days (a month)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>For example, if <strong>inv_rate_type=3</strong> and <strong>inv_rate_value=5</strong>, the software scan repeats every 5 months.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> To preserve the consistency of software scan statuses configure scan schedules through the web UI. Changing this parameter separately might result in the <strong>Missing software scan</strong> status.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>inv_rate_value</strong></td>
<td>integer</td>
<td>1</td>
<td>1</td>
<td>9999</td>
<td>All</td>
</tr>
<tr>
<td>Description</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>The number of repeating periods, as defined by <strong>inv_rate_type</strong>, that separate the consecutive occurrences of the software scan.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> To preserve the consistency of software scan statuses configure scan schedules through the web UI. Changing this parameter separately might result in the <strong>Missing software scan</strong> status.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Parameter</td>
<td>Units</td>
<td>Default</td>
<td>Minimum</td>
<td>Maximum</td>
<td>Supported agents</td>
</tr>
<tr>
<td>-----------------------</td>
<td>-----------</td>
<td>---------</td>
<td>---------</td>
<td>---------</td>
<td>-----------------------------------------</td>
</tr>
<tr>
<td><strong>inv_start_date</strong></td>
<td>date</td>
<td></td>
<td></td>
<td></td>
<td>All</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The date of inclusion in the database.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>The date and time when the first or only occurrence of the software inventory scan is performed. The format is YYYY-MM-DD.hh.mm.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Note:</strong> To preserve the consistency of software scan statuses configure scan schedules through the web UI. Changing this parameter separately might result in the <strong>Missing software scan</strong> status.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>native_scan_enabled</strong></td>
<td>Boolean</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>Tivoli Asset Discovery for Distributed 7.2 and higher</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Enables scanning native registry during a software scan so that the agents start uploading information about unmatched registry software to the server.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>ping_period</strong></td>
<td>minutes</td>
<td>60</td>
<td>60</td>
<td>360</td>
<td>All</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The length of time the agent waits between checks of the connection to the server when the connection is not available.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>proc_list_period</strong></td>
<td>seconds</td>
<td>300</td>
<td>60</td>
<td>600</td>
<td>All</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The frequency with which the agent checks the list of running processes for applications use monitoring.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>remote_scan_enabled</strong></td>
<td>Boolean</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>Tivoli Asset Discovery for Distributed 7.2 and higher</td>
</tr>
<tr>
<td></td>
<td></td>
<td>It determines whether the agents must scan remote file systems. If the value is 0, the agents detect the disks but they do not scan them. If the value is 1, the disks are scanned.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Note:</strong> You can enable or disable the parameter only on the -all level.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>scan_priority</strong></td>
<td>integer</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>All</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Determines the priority of scan-related processes (hardware, capacity, and software scans). You can use it to lower the priority of the scans so as not to overload your servers. The possible values are:</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>0 Low priority</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>1 Normal priority</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>2 High priority</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>service_timeout</strong></td>
<td>seconds</td>
<td>30</td>
<td>30</td>
<td></td>
<td>All</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Determines the time the agent waits for the response from the server.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>sw_scan_timeout</strong></td>
<td>minutes</td>
<td>720</td>
<td>60</td>
<td></td>
<td>Tivoli Asset Discovery for Distributed 7.2.1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The maximum period in which the software scan process should finish. Otherwise, the agent reports an error. As the software scan process consists of both the scanning and some additional evaluation, the overall software scan time might exceed the value provided.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>sys_update_period</strong></td>
<td>minutes</td>
<td>30</td>
<td>30</td>
<td>10080 (1 week)</td>
<td>All</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Defines the frequency of the scanning processor.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>update_enabled</strong></td>
<td>integer</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>All</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Indicates the status of the agent self-update service. The possible values are:</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>0 Disabled.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>1 Periodic: agents check for new versions at regular periods defined by the update_period parameter.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>2 Scheduled: agents check for new versions during a period defined by the start date specified by the update_start parameter and the length of the update period defined by the update_interval parameter.</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Table 5. Agent configuration parameters (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Units</th>
<th>Default</th>
<th>Minimum</th>
<th>Maximum</th>
<th>Supported agents</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>parameter</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>update_interval</td>
<td>hours</td>
<td>6</td>
<td>1</td>
<td>24</td>
<td>All</td>
</tr>
<tr>
<td>update_period</td>
<td>minutes</td>
<td>10080 (1 week)</td>
<td>1440 (1 day)</td>
<td>129600 (3 months)</td>
<td>All</td>
</tr>
<tr>
<td>update_start</td>
<td>date</td>
<td>The date of inclusion in the database.</td>
<td>All</td>
<td></td>
<td></td>
</tr>
<tr>
<td>upload_unk_period</td>
<td>minutes</td>
<td>180</td>
<td>180</td>
<td>Tivoli License Compliance Manager</td>
<td></td>
</tr>
<tr>
<td>upload_usage_period</td>
<td>minutes</td>
<td>360 (6 hours)</td>
<td>180 (3 hours)</td>
<td>10080 (1 week)</td>
<td>All</td>
</tr>
<tr>
<td>use_scan_enabled</td>
<td>Boolean</td>
<td>1</td>
<td>0</td>
<td>All</td>
<td></td>
</tr>
<tr>
<td>use_snapshot_period</td>
<td>seconds</td>
<td>300</td>
<td>60</td>
<td>600</td>
<td>All</td>
</tr>
<tr>
<td>use_report_period</td>
<td>minutes</td>
<td>1440 (1 day)</td>
<td>180 (3 hours)</td>
<td>10080 (1 week)</td>
<td>All</td>
</tr>
<tr>
<td>virtual_hw_scan_disabled</td>
<td>Boolean</td>
<td>no</td>
<td>no</td>
<td>All</td>
<td></td>
</tr>
<tr>
<td>was_check_period</td>
<td>minutes</td>
<td>1440 (1 day)</td>
<td>120 (2 hours)</td>
<td>2880 (2 days)</td>
<td>All</td>
</tr>
</tbody>
</table>

**Setting processor consumption limits on agents**

This functionality defines the processor consumption time limit that is available for the Common Inventory Technology component, which is run by agents during...
software scans. The `cpu_threshold` parameter can have the value 5-100, and is the allocated processor time limit that should not be exceeded when the software scan or other CPU-intensive operations are performed by the agent.

**Before you begin**

- You must have the following operating system privileges:
  - Windows: Administrator
  - UNIX: root
- The command-line interface must be able to connect to the server using address "localhost".
- Security must be enabled on the server.

**About this task**

- **Interim Fix 4**: Starting from interim fix 4, the `cpu_threshold` parameter functionality is extended. In addition to limiting the CPU consumption of the software scan, it also limits the CPU consumption of the use scan and hardware scan.

**Procedure**

1. Access the command-line interface.
2. Log in to the server.
3. At the command line, type the `setagentconf` command with the following options:
   ```
   -d scan_group_name -k cpu_threshold -v value
   ```
   Where
   ```
   value
   ```
   is the maximum processor consumption time (expressed in percents) of the Common Inventory Technology component on selected agents. It takes the values 5-100.

   Example: To set the `cpu_threshold` parameter to 10 on the agents in Europe scan group, enter:
   ```
   setagentconf -d Europe -k cpu_threshold -v 10
   ```

**Enabling the agent self-update**

You can enable the agents to selfupdate using the `setagentconf` command on all platforms except IBM i, Solaris local zones, and Solaris global zones (with existing local zones). The Self-update of Tivoli Asset Discovery for Distributed agents allows you to upgrade them without changing their configuration parameters. You can enable them to self-update automatically whenever a fix pack or a new version is released.

**About this task**

Agent self-updates are based on the local time zones in which agents are located and not the time on the Tivoli Asset Discovery for Distributed server. This is important if you are managing computers from distant locations, for example, on different continents. For example, if you schedule the agents to download and install updates at midnight (in different time zones), it will result in agents contacting the server at different times (relative to the server time).
For large environments, especially the ones approaching the maximum number of agents for one server, performance problems may occur while the agents are being updated. To avoid that, you can schedule the update for different scan groups at different times. See the setagentconf command in the Commands section of the information center.

On AIX®, the main usr directory on an LPAR can be shared with WPARs. If the directory is not shared, the agents will be updated on the LPAR and the WPARs. If it is shared, it means that agents installed on WPARs can have read-only access to the usr directory and the agent on the LPAR gets updated first, while the agents on WPARs are updated only after the agent files on the LPAR have been updated.

Note: Agent self-update is not supported on the following platforms:

- HP-UX 11i for PA-RISC
- IBM i
- Linux with kernel version 2.4.21-47
- Solaris local zones, and global zones (with existing local zones). It is also not supported on Solaris 10 if the agent was installed with -G flag by using the shell installer.

Important: Self-update packages are signed by using public-key infrastructure (PKI).

Procedure

1. Log on to the Tivoli Asset Discovery for Distributed server command-line interface.

2. To enable the agents self-update enter the setagentconf command: \{ -d scanGroup | -all \} -k update_enabled -v value -s active, where:

   -d scanGroup
   The name of the scan group for which the configuration is being set (i.e. configuration will be set for the whole scan group rather than particular agents).

   -all
   Sets the configuration key for all agents.
   You might also want to enable self-update only for a specific scan group (This is an example only).

   -k update_enabled
   Required. Specifies the name of the agent configuration parameter.

   -v value
   Specifies if the self-update facility is enabled. Possible values are:
   • 0 - disabled.

   Note: If you disable the self-update functionality (the setagentconf command for the update_enabled parameter with value 0), all previously set parameters regarding agent self-update (update_period, update_start and update_interval) are reset to their default values.
   • 1 - enabled periodic update. For information about how to set the frequency see Configuring a periodic agent self-update.
- 2 - enabled update in time frame. For information about how to set the start date and time frame see Configuring a scheduled agent self-update.

-s active
Specifies the state of the configuration parameter. When it is set to active, the value of the parameter is used.

Note: During the self-update from IBM Tivoli License Compliance Manager Fix Pack 4 and 5 on Windows, the wd1ssp command fails and the self-update ends with no action. To avoid this problem:

a. Stop the agent with the tlmagent -e command.
b. Open Start > Control Panel > Administrative Tools > Services > Tivoli Asset Discovery for Distributed Agent.
c. Go to the Logon tab.
d. Clear the Allow service to interact with desktop option and click OK.
e. Start the agent with the tlmagent -g command.

Results
During the next download of agent parameters, each agent checks the server for a changed version of the agent deployment package for its operating system. The interval between checks is defined by the update_period parameter. In case of scheduled self-update it is defined by the starting date and the length of the period during which the agent picks up a random date for contacting the server.

When a new version of the package is found, the agent downloads it and applies the changes. The changes can relate to the agent itself or to one of its corequisites.

What to do next
When all agents have been upgraded disable the self-update by setting the update_enabled parameter to hold.

Important:

For AIX and Solaris, the dependency scan works only if the ls of 4.80 diagnostic tool is installed. The default ls of installation path is /usr/sbin/ls of. If you choose an installation path other than the default, you must issue the wscancfg -s ls of.bin PATH_TO_LSOF_BINARY command.

For example, for Common Inventory Technology installed in a default location:

```
/opt/tivoli/cit/bin/wscancfg -s ls of.bin /opt/sbin/ls of
```

will instruct Common Inventory Technology to use ls of located in /opt/sbin/.

To download ls of 4.80, visit the following websites and search for the ls of packages:

- AIX Web Download Pack Programs
- Sunfreeware website

Tip: Dependency scans work if the following commands can be executed with the ls of you installed:

1. ls of -14 -i6 -P -n (for AIX, Solaris 8 and Solaris 9)
2. `ls/of -z -i4 -i6 -P -n` (for Solaris 10 and Solaris 11)
   Solaris 10 requires the following versions of `ls/of`:
   - Solaris 10 05/08 or higher requires `ls/of` 05/08 4.80
   - Solaris 10 11/06 with a patch applied to the kernel requires `ls/of` 05/08 4.80
   - Solaris 10 11/06 or lower requires `ls/of` 11/06 4.80

**Configuring a scheduled agent self-update**

Agent parameters `update_start` and `update_interval` allow you to define a time window during which the agent self-update can be performed.

**About this task**

Agents are able to identify the time window that has been set for updates and contact the administration server during that period.

Like the other agent parameters, the agent self-update settings can be applied at the agent level. This provides more flexibility, allowing you to plan a staged upgrade of a group of agents and to ensure that the update processing takes place at a time that is convenient to you.

**Note:** It is important to remember that on certain operating systems the self-update time frame must be reasonably wide, stretching even a few days. The length of the time frame largely depends on the frequency and length of software scans.

The following scenario demonstrates how to schedule the update of agents in the Sales scan group to take place between 22:00 on 10th July 2011 and 6.00 on the 11th July 2011.

**Procedure**

1. Issue the following command to enable self-update in a time frame for agents in the Sales scan group.

   ```
   setagentconf -d Sales -k update_enabled -v 2 -s active
   ```

2. Issue the following command to start the update period at 22:00 on 10th July 2011.

   ```
   setagentconf -d Sales -k update_start -v 2011-07-10-22.00 -s active
   ```

3. Issue the following command to end the update period at 6.00 on the 11th July 2011, by setting the update period to 8 hours.

   ```
   setagentconf -d Sales -k update_interval -v 8 -s active
   ```

   **Note:** The exact time of starting the update is chosen randomly within the specified timeframe. Such an approach provides you with an automatic mechanism of load balancing and prevents from overloading the server by many agents, which might attempt to perform self update at the same time.

**Configuring a periodic agent self-update**

When the periodic update option is enabled, agents check the administration server for updates at regular intervals defined by the `update_period` parameter.
About this task

The default value for this parameter is 10080 minutes (one week). If you have performed a proof-of-concept installation, you can set the parameter to any value that you find appropriate. For production environment, the minimum value is 1440 minutes (one day), and the maximum is 129600 (90 days).

Procedure
1. Issue the following command to enable periodic self-update for agents in the Sales scan group.

   ```bash
   setagentconf -d Sales -k update_enabled -v 1 -s active
   ```

2. To set the frequency of the self-update for the agents in the Sales scan group for 1440 minutes, issue the following command:

   ```bash
   setagentconf -d Sales -k update_period -v 1440 -s active
   ```

Implementing and removing a test configuration

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

About this task

The values are set for the Sales scan group and override the values already set. The configuration is prepared in advance, put on hold and then later activated.

Procedure
1. Issue the following commands to define the new configuration values, put them on hold.

   ```bash
   setagentconf -d Sales -k upload_usage_period -v 360 -s hold
   setagentconf -d Sales -k down_parms_period -v 360 -s hold
   ```

2. Issue the following command to activate the settings.

   ```bash
   setagentconf -d Sales -k upload_usage_period -s active
   setagentconf -d Sales -k down_parms_period -s active
   ```

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

   ```bash
   setagentconf -d Sales -k upload_usage_period -s hold
   setagentconf -d Sales -k down_parms_period -s hold
   ```

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

Configuring SELinux to work with the agent

If you are using Security Enhanced Linux, you can configure it so that the Tivoli Asset Discovery for Distributed agent gathers the required data. The configuration is supported on Red Hat Enterprise Linux version 5.0 and higher with SELinux enabled in the enforcing mode with Policy version 21 or higher and a targeted policy type.
Before you begin

- The Tivoli Asset Discovery for Distributed agent must be installed on the target computer and started by a root user.

**Tip:** If you encounter problems during the installation of an agent on a computer with SELinux enabled, they might be caused by GSKit binary files. The files cannot run under SELinux when text relocation is enabled. To turn off text relocation in the GSKit package, change to the agent directory and run the following command:

```
setsebool -P allow_execmod=1 ./tlmagent
```

**Tip:** If you encounter problems with starting the agent, ensure that all libraries that are used by the agent have the file context set to textrel_shlib_t. To change the file context of a library, run the following command:

```
chcon -t textrel_shlib_t /path_to_lib/libname.so
```

Where `path_to_lib` is a path to the agent library, and `libname` is the name of the library.

- The policycoreutils-python package must be installed on the computer.
- On Red Hat Enterprise Linux 5.0, the root user must be mapped to the SELinux user who has the following roles: `system_r`, `sysadm_r`, and `user_r`. On Red Hat Enterprise Linux 6.0 and higher, the root user must be mapped to the SELinux user who has the following roles: `system_r` and `unconfined_r`.

About this task

The agent is compatible with SELinux in the enforcing mode on Red Hat Enterprise Linux version 5.0 and higher with SELinux Policy at least version 21 and a targeted policy type.

Procedure

1. Log in to the agent computer as a root user.
2. To check what is the mode and policy type of SELinux, run the following command:

```
sestatus
```

If SELinux is enabled in the enforcing mode with policy version at least 21 and targeted policy type, the command returns the following output:

```
SELinux status: enabled
SELinuxfs mount: /selinux
Current mode: enforcing
Mode from config file: enforcing
Policy version: 21
Policy from config file: targeted
```

3. Ensure that the agent process has the following security context format:

```
root:system_r:unconfined_t
```

To check the security context format, run the following command:

```
ps auxZ |grep tlmagent
```

4. After the first hardware scan is run on the agent, check the SELinux log file for AVC messages. For example:

```
type=AVC msg=audit(1398425753.491:44): avc: denied { read write } for pid=2412 comm="/ifconfig" path="/var/itlm/scanner/tml_hw_output.gz" dev=sdafino=278703 scontext=system_u:system_r:ifconfig_t:s0 tcontext=system_u:object_r:var_t:s0 tclass=file
```
The messages are logged only if the Linux Auditing System is enabled. By default, the audit.log file is in the /var/log/audit directory. If there are no AVC messages in the log, the agent should work properly and no additional steps are required. If AVC messages exist in the log, proceed to step 5.

5. To generate a module that contains policy rules, which allow for assigning the agent with appropriate rights, run the following command:

```
grep -i 'cit\|wscan\|tlmagent\|vmware-rpctool\|itlm' /var/log/audit/audit.log | audit2allow -M lmtmodule
```

6. To install the module, run the following command:

```
semodule -i lmtmodule.pp
```

7. To check whether the module was successfully installed, run the following command:

```
semodule -l
```

If the command output lists an lmtmodule, the module was successfully installed.
Appendix.

Review the following additional information before you configure IBM License Metric Tool
Tivoli Asset Discovery for Distributed.

Starting the server

To start the server, you must run the srvstart.bat or srvstart.sh script. If the server does not start after running the script, you must start the DB2 instance and rerun the script.

Before you begin

- You must have the following operating system privileges to start the server:
  - UNIX/Linux: root
  - Windows: Administrator.

Procedure

1. Go to the directory <INSTALL_DIR>/cli, where <INSTALL_DIR> is the name of the Tivoli Asset Discovery for Distributed installation directory.
2. Run the following script:
   - Windows: srvstart.bat
   - UNIX: srvstart.sh
3. Optional: If your server does not start after running the script, you must start your DB2 instance. By default, DB2 instances that were created during the installation on the Windows operating system are set to autostart. To set up DB2 to autostart, do the following steps:
   a. Log on to the computer where DB2 is installed with the DB2 administrator ID and password that were specified at the installation time.
   b. UNIX: On UNIX computers, run the following script:
      $INSTHOME/sqllib/db2profile
   c. Type db2start at the command line. The DB2 instance starts.
   d. Stop the server and start it by repeating steps 1 and 2.

Stopping the server

When you are stopping the server, you might also consider stopping the DB2 database software.

Before you begin

- You must have the following operating system privileges to stop the server:
  - UNIX/Linux: root
  - Windows: Administrator.

Procedure

1. Go to the directory <INSTALL_DIR>/cli, where <INSTALL_DIR> is the name of the Tivoli Asset Discovery for Distributed installation directory.
2. Run the srvstop.bat (Windows) or srvstop.sh (UNIX) script.
Tip: On Linux and UNIX, you are prompted for the user administrator ID and password. Optionally, you can use the parameters `-username` and `-password` when you run the `srvstop.sh` script.

The server stops.

3. Additionally, you may want to stop the DB2 instance.
   a. Log in to the machine where DB2 is installed with the DB2 administrator ID and password specified at installation time.
   b. Type `db2stop` at a DB2 command line.

The DB2 instance stops.
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.

---

**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.

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.
Index

A
administration server
configuring 13
registering 19
server 19
agent
parameters
configuring 19
agent parameters
configuring 19
agents
configuration commands 21
configuring 19
inactive 16
self-updates
configuring periodic
self-updates 30
scheduling 29
settings 22
updating 26

L
log.properties
files 18
trace parameters
configuring 18
log.properties file 18

M
mail settings
configuring 8
server settings 8
maxPdfRows parameter 16

N
notifications
configuring 8

P
parameters
server database 13
part numbers
importing 6
uploading 6
pricing model
tier-based 6
privacy policy
defining 17
processor value units (PVU) table
importing 5
processor value units (PVUs)
importing 5
PVU (processor value units) table
importing 5
PVUs (processor value units)
importing 5

R
recipients
event notifications 8
registration
server 19
service 19

S
scenarios
self-updates 29
security
defining FIPS 140-2 server
encryption 13
user permissions 2
self-update service
scheduling 29

T
tcr
configuring 10
test configuration
implementing 30
tivoli common reporting
configuring 10
transaction log size
configuring 18

U
user permissions
configuring 2
users
adding 2
defining privacy policy 17

V
virtual machine managers
adding 8
vm managers
adding 8
kvm 8
microsoft hyper-v 8
vmware vsphere 8
websphere cloudburst 8

W
Web user interface 13