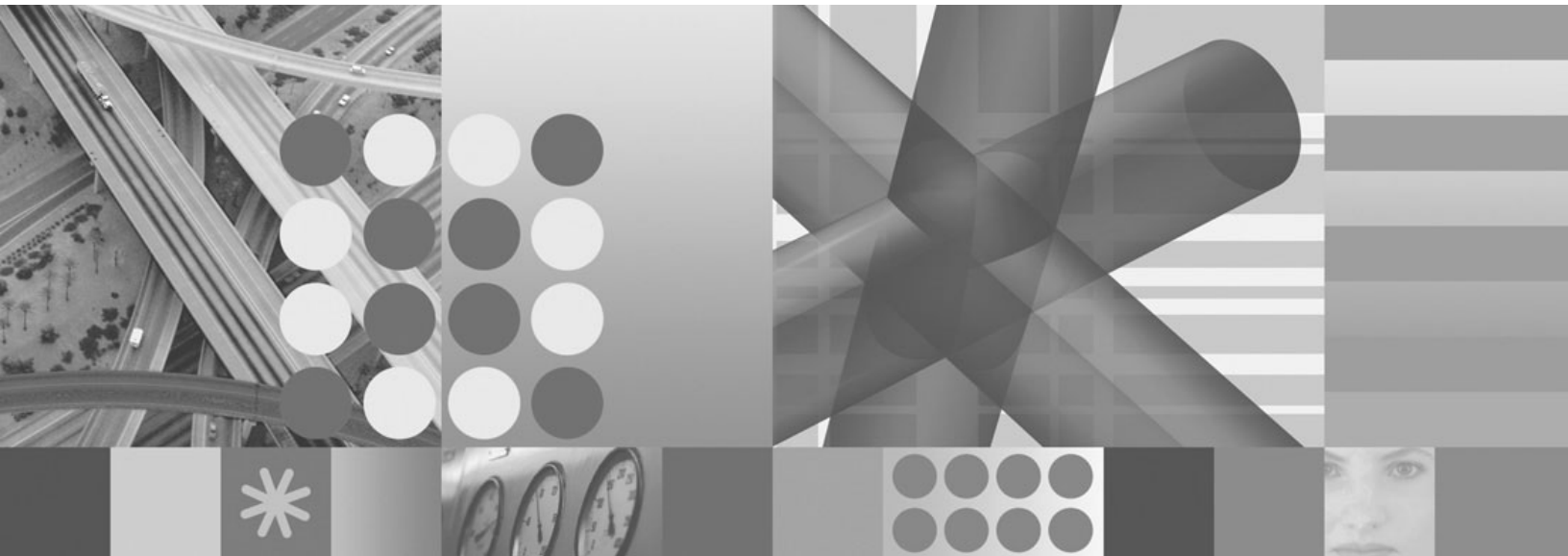




LDAP Data Model Conversion Utility



LDAP Data Model Conversion Utility

Note

Before using this information and the product it supports, read the information in "Notices" on page 31.

First Edition (January 2006)

This edition applies to version 6, release 0, modification 0 of IBM Tivoli Access Manager (product number 5724-C08) and to all subsequent releases and modifications until otherwise indicated in new editions.

© Copyright International Business Machines Corporation 2006. All rights reserved.

US Government Users Restricted Rights – Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

Contents

Chapter 1. Introduction	1	Chapter 5. Conversion procedures.	13
Chapter 2. Upgrade considerations	3	Procedures when not reinstalling the LDAP server	14
Chapter 3. Purpose of utility	5	IBM Tivoli Directory Server procedure	14
High-level process	5	Sun Java System Directory Server procedure	16
amldif2v6 syntax	6	Novell eDirectory procedure.	18
Novell eDirectory differences	6	Procedures when reinstalling the LDAP server	20
Associated utilities for Novell eDirectory	6	IBM Tivoli Directory Server procedure	20
Novell eDirectory high-level process	7	Sun Java System Directory Server procedure	21
Chapter 4. Managing user and group		Novell eDirectory procedure.	23
definitions for the conversion	9	Chapter 6. Installation	27
Creating the input file and importing the output file	9	Chapter 7. Performance	29
IBM Tivoli Directory Server procedure.	9	Overall performance	29
Sun Java System Directory Server procedure.	9	Improving conversion tool-specific performance	29
Novell eDirectory procedure	9	Determining the size of the in-memory user cache	30
Deleting LDAP objects before importing the output		The data-conversion processes	30
file	10	Notices	31
IBM Tivoli Directory Server procedure	10	Trademarks	32
Sun Java System Directory Server procedure	10		
Novell eDirectory procedure.	11		

Chapter 1. Introduction

IBM® Tivoli® Access Manager supports several types of registries to contain user and group definitions. Tivoli Access Manager can use these definitions for authentication and authorization. One of the supported registry types is Lightweight Directory Access Protocol (LDAP). Many vendors provide LDAP products and Tivoli Access Manager supports several natively, including IBM Tivoli Directory Server, Sun Java™ System Directory Server, and Novell eDirectory Server. In all cases, the IBM Tivoli Directory Server client is used by Tivoli Access Manager as the client-side interface providing LDAP protocol access. See the *IBM Tivoli Access Manager for e-business: Release Notes*, version 6.0, for the list of supported vendors and product versions.

Many Tivoli Access Manager customers require large numbers of user definitions (a million or more) in their registry. The current data model (the way the Tivoli Access Manager data is created and maintained in the LDAP server) requires up to four objects per user plus the standard person definition. Optionally with Tivoli Access Manager 6.0, new customers will be able to take advantage of a new Tivoli Access Manager LDAP data model. With the new model, the number of required objects per user is reduced to only one plus the standard person definition. The new data model provides the following benefits:

- A reduced “footprint” for the data model
- A lesser amount of LDAP server storage required for each user definition, which gives you the ability to maintain larger numbers of user definitions

Newly installed and configured Tivoli Access Manager 6.0 systems will use the new LDAP data model by default. Existing Tivoli Access Manager customers who upgrade to Tivoli Access Manager 6.0 might also want to take advantage of the benefits of the new data model.

Tivoli Access Manager 6.0 provides a utility that will help customers who are upgrading to 6.0 convert the Tivoli Access Manager data that they store in their LDAP user registries to the new data model. This utility, its associated utilities, and the supporting documentation are not shipped with Tivoli Access Manager 6.0. Instead, customer need to access and download the utility and documentation from the following Web address:

<http://www.ibm.com/software/sysmgmt/products/support/IBMTivoliAccessManagerfore-business.html>

Conversion to the new data model can be performed regardless of whether the LDAP server is IBM Tivoli Directory Server, Sun Java System Directory Server, or Novell eDirectory and regardless of the number of user and group definitions in use by Tivoli Access Manager.

Conversion to the new data model is completely optional. A Tivoli Access Manager system that has been upgraded to Tivoli Access Manager 6.0 will continue to work with the previous data model. Customers who choose to convert to the new data model are strongly encouraged to attempt this conversion with support from either the Tivoli Access Manager service team or with the IBM Software Support that is provided under their services contract.

Chapter 2. Upgrade considerations

All Tivoli Access Manager components in the enterprise should be upgraded to the 6.0 release before considering converting to the 6.0 LDAP data model. See the *IBM Tivoli Access Manager for e-business: Upgrade Guide*, version 6.0, for information about upgrading Tivoli Access Manager to version 6.0. After the data model has been converted, previous versions of Tivoli Access Manager can no longer be used. It is recommended that the customer enlist IBM Software Support to assist with the data conversion.

With the two systems policy server upgrade method, the data model cannot be converted until all components of Tivoli Access Manager in the enterprise are upgraded and the original previous version of the policy server is removed.

Upgrading the data model is not recommended for Tivoli Access Manager environments in which the number of LDAP user definitions is small.

Chapter 3. Purpose of utility

Customers who are installing and configuring the Tivoli Access Manager 6.0 product for the first time automatically take advantage of the new LDAP data model for user and group definitions by default. For these customers, there is no LDAP data model conversion to be preformed.

The utility is only for those customers who are already Tivoli Access Manager customers and have an existing pre-version 6.0 Tivoli Access Manager configuration. These customers need to make the following choice:

- Continue to use their existing LDAP databases, and, thereby, continue to use the old LDAP data model for user and group definitions
- Convert their existing LDAP databases to the new LDAP data model

Customers who need to continue to support versions of Tivoli Access Manager before version 6.0 in their environment should not take advantage of the new data model. These customers should not attempt the LDAP data model conversion that is described in this document.

For customers who choose to convert their existing LDAP databases, Tivoli Access Manager provides the **amldif2v6** data model conversion utility. This utility accepts as input a file that contains an LDIF representation of the entire LDAP database for that customer. From this input LDIF file, the **amldif2v6** creates an output LDIF file that represents the entire LDAP database for the customer and incorporates the modifications to the Tivoli Access Manager data required by the new data model.

LDAP objects in the input LDIF file that were not created by Tivoli Access Manager are copied to the output LDIF file unmodified. The customer will use the output LDIF file to recreate completely the LDAP database. The output LDIF file will be imported using native LDAP tools that are described later in this document.

Note: LDAP Data Interchange Format (LDIF) is a standard text representation for LDAP data. This standard was created to provide a simple and versatile way for data to be transferred between LDAP servers on various operating system platforms. All LDAP servers provide tools for exporting objects in LDIF format from their databases and for importing objects in LDIF format into their databases.

High-level process

At a high level, the LDAP data model conversion process consists of the following tasks:

- Use native LDAP tools to export the entire contents of the LDAP database to an LDIF file. This LDIF file will be the input LDIF file for the **amldif2v6** utility.
- Use the **amldif2v6** utility to process the input LDIF file and to produce a file in which many of the Tivoli Access Manager-created objects are modified in accordance with the new Tivoli Access Manager LDAP data model.
- Use native LDAP tools to delete the entire contents of the LDAP database.
- Use native LDAP tools to import the contents of the output LDIF file that was generated by the **amldif2v6** utility.

Attention: The high-level process for Novell eDirectory Server differs slightly. For complete details, see “Novell eDirectory differences.”

amldif2v6 syntax

The invocation syntax of the **amldif2v6** utility:

```
amldif2v6 input_LDIF_filename output_LDIF_filename max_user_cache_entries
max_group_cache_entries [debug_filename]
```

input_LDIF_filename

Specifies the file containing an LDIF representation of the customer's LDAP database.

output_LDIF_filename

Specifies the file to receive the LDIF output of the utility.

max_user_cache_entries

Specifies the maximum number of entries to be allocated within the in-memory user cache.

max_group_cache_entries

Specifies the maximum number of entries to be allocated within the in-memory group cache.

debug_filename

Specifies the optional name of the debug file. With this option, the utility writes debug trace information to the specified file as it runs.

Novell eDirectory differences

The LDAP data model conversion process is slightly different when using Novell eDirectory Server. Novell eDirectory does not allow the `userPassword` attribute of a person object to be exported to LDIF. Therefore, it is not possible to export the entire Novell eDirectory database to an LDIF file. Without the `userPassword` attribute, all user password information would be lost.

Instead of extracting the entire contents of the Novell eDirectory LDAP database to an LDIF file, only those Tivoli Access Manager objects that are impacted by the data model change will be extracted. Correspondingly, instead of deleting the entire contents of the LDAP database before importing the generated output LDIF file, only those Tivoli Access Manager objects that are impacted by the data model change will be deleted.

Associated utilities for Novell eDirectory

To assist you with these tasks, Tivoli Access Manager provides the following associated utilities:

getamobjects

The associated utility that obtains the LDIF representation the Tivoli Access Manager LDAP objects that are impacted by the data model change.

deleteamobjects

The associated utility that deletes the Tivoli Access Manager LDAP objects that will be replaced by the objects contained in the output LDIF file that was generated by the **amldif2v6** utility. The **deleteamobjects** utility does not delete person objects.

Each of these utilities requires some manual editing by the customer before use. Follow the instructions contained within each utility.

Novell eDirectory high-level process

At a high level, the LDAP data model conversion process for Novell eDirectory Server will proceed as follows:

1. Use the **getamobjects** utility to export the Tivoli Access Manager objects that are impacted by the data model change. This will be the input LDIF file for the **amldif2v6** utility.
2. Use the **amldif2v6** utility to process the input LDIF file and produce a file in which those objects have been modified in accordance with the new LDAP data model.
3. Use the **deleteamobjects** utility to delete the Tivoli Access Manager objects that will be replaced by the objects in the output LDIF file that was generated by the **amldif2v6** utility.
4. Use native LDAP tools to import the contents of the LDIF file.

Chapter 4. Managing user and group definitions for the conversion

To convert user and group definitions to the new Tivoli Access Manager data model, you need to perform the following tasks:

- Create the input LDIF file for the **amldif2v6** utility
- Delete objects from the LDAP server before importing the output LDIF file that the **amldif2v6** utility generated
- Import the output LDIF file that the **amldif2v6** utility generated

Creating the input file and importing the output file

The actual conversion procedure is described in detail in Chapter 5, “Conversion procedures,” on page 13. This section introduces you to the tools that you should use to create the input LDIF file for the **amldif2v6** utility and the tools that you should use to import the output LDIF file that was generated by the **amldif2v6** utility.

IBM Tivoli Directory Server procedure

To create the input LDIF file, use the **Export LDIF Data** function of the IBM Tivoli Directory Server Configuration Tool.

To import an output LDIF file that contains 10000 users or fewer, use the **ldapadd** command to import the file. Otherwise, follow the instructions within the *IBM Tivoli Access Manager: Performance Tuning Guide* for importing large LDIF files.

Refer to the appropriate product documentation to obtain usage instructions for these tools.

Sun Java System Directory Server procedure

To create the input LDIF file, use the **Export Databases** function of the Sun Directory Server Console.

To import the output LDIF file, use the **Import Databases** function of the Sun Directory Server Console.

Refer to the appropriate product documentation to obtain usage instructions for these tools.

Novell eDirectory procedure

To create the input LDIF file, use the Tivoli Access Manager **getamobjects** utility. This utility requires manual editing before use. Follow the instructions contained in the utility.

To import the output LDIF file, use the Novell eDirectory ConsoleOne Import/Export Wizard.

Refer to the appropriate product documentation to obtain usage instructions for these tools.

Deleting LDAP objects before importing the output file

The actual conversion procedure is described in detail in Chapter 5, “Conversion procedures,” on page 13. This section introduces you to the tools that you should use to delete objects from the LDAP server before importing the output LDIF file that was generated by the **amldif2v6** utility.

IBM Tivoli Directory Server procedure

When using IBM Tivoli Directory Server, make one of the following choices:

- Assuming that the entire LDAP database was copied to the input LDIF file, the quickest way to delete these objects from the LDAP server is to perform the following procedures:
 1. Use the IBM Tivoli Directory Server Configuration Tool to unconfigure and destroy the database
 2. Re-configure a new database
 3. Use the IBM Tivoli Directory Server Configuration Tool to recreate, but not instantiate, all suffixes which were present in the input LDIF file
 4. Restart the LDAP server

Most customers are expected to use this method.

- Assuming that the entire LDAP database was copied to the input LDIF file, another alternative for deleting these objects from the LDAP server is to perform the following procedures:
 1. Uninstall IBM Tivoli Directory Server and DB2®
 2. Delete the DB2 database
 3. Reinstall DB2 and IBM Tivoli Directory Server
 4. Use the IBM Tivoli Directory Server Configuration Tool to recreate, but not instantiate, all suffixes which were present in the input LDIF file
 5. Restart the LDAP server
- Another alternative is to perform the following procedures:
 1. Remove IBM Tivoli Directory Server from the network,
 2. Install a new IBM Tivoli Directory Server from scratch on a new system
 3. Modify the TCP/IP configuration of the new system to replace the machine that was removed
 4. Use the IBM Tivoli Directory Server Configuration Tool to recreate, but not instantiate, all suffixes which were present in the input LDIF file
 5. Restart the LDAP server

Sun Java System Directory Server procedure

When using Sun Java System Directory Server, make one of the following choices:

- Assuming that the entire LDAP database was copied to the input LDIF file, the Sun Directory Server Console provides a similar capability for deleting an LDAP database. From the Sun Directory Server Console perform the following procedures:
 1. On the **Configuration** tab, expand the **Data** element in the left-hand column and select the suffix to be deleted
 2. Click the **Databases** tab, and select the database associated with this suffix
 3. Click on **Delete**.

Note: Each suffix should be deleted except for cn=NetscapeRoot. If this suffix is deleted, the Sun Java System Directory Server will not function properly.

4. Right click the **Data** element in the left-hand column to recreate, but not instantiate, each suffix present in the input LDIF file
 5. Restart the LDAP server
- Assuming that the entire LDAP database was copied to the input LDIF file, another alternative for deleting these objects is to perform the following procedures:
 1. Uninstall and reinstall the Sun Java System Directory Server.
 2. Use the Sun Directory Server Console to recreate, but not instantiate, each suffix present in the input LDIF file
 3. Restart the LDAP server.
 - Another alternative is to perform the following procedures:
 1. Remove the Sun Java System Directory Server from the network
 2. Install a new Sun Java System Directory Server from scratch on a new system
 3. Modify the TCP/IP configuration of the new system to replace the machine that was removed
 4. Use the Sun Directory Server Console to recreate, but not instantiate, each suffix present in the input LDIF file
 5. Restart the LDAP server

Novell eDirectory procedure

To delete all of the Tivoli Access Manager LDAP objects that will be replaced by the objects contained within the **amldif2v6** output LDIF file, use the Tivoli Access Manager **deleteamobjects** utility.

Note: This utility does not delete any person object.

This utility requires manual editing before use. Follow the instructions contained in the utility.

Chapter 5. Conversion procedures

It is not mandatory that existing Tivoli Access Manager customers convert their LDAP data to the new data model. The old Tivoli Access Manager LDAP data model will continue to be supported and customers should not see any difference if they choose to retain this data model after upgrading to Tivoli Access Manager, version 6.0.

Existing Tivoli Access Manager customers might choose to convert their environment to the new data model to take advantage of the fewer LDAP objects that are required for each user or group definition. Fewer LDAP objects result in a savings of storage space on the LDAP server. Customers also might choose to convert to the new data model to eliminate the need to store Tivoli Access Manager-specific LDAP objects below the user or group base object definitions. The storage of the Tivoli Access Manager-specific LDAP objects is a concern for Novell eDirectory customers, because this location means that the person definition is no longer a *leaf* object.

Attention: Before converting Tivoli Access Manager LDAP data to the minimal data model, ensure that no other product in the enterprise uses a pre-6.0 version of the Tivoli Access Manager runtime. After the conversion, any product which used the previous versions of the Tivoli Access Manager runtime, will no longer be supported. Products that depend on the Tivoli Access Manager runtime include WebSeal, IBM Tivoli Access Manager for Operating Systems, IBM Tivoli Access Manager for Business Integration or other Tivoli Access Manager blades. If previous versions of these products exist in the enterprise, they must be upgraded to version 6.0 before converting the LDAP data model. After determining that no previous versions of a product in the enterprise has a dependency on a pre-6.0 version of the Tivoli Access Manager runtime and after deciding that the savings with the minimal data model are desirable, you can use the conversion utility to convert the data to the new data model.

If a customer decides that converting the Tivoli Access Manager LDAP data to the new LDAP data model is desirable, the customer needs to choose which of the following approaches to adopt:

- The first conversion procedure describes how to perform the data conversion when the LDAP server does not need to be reinstalled. In other words, the customer wants to retain the current LDAP server because it is still compatible with Tivoli Access Manager, version 6.0. This approach is discussed in “Procedures when not reinstalling the LDAP server” on page 14.
- The second conversion procedure describes how to perform the data conversion when the LDAP server needs to be reinstalled. The LDAP server might need to be reinstalled because the version of the LDAP server is no longer compatible with Tivoli Access Manager, version 6.0, or because the customer wants to upgrade to a more recent version of that LDAP server. This approach is discussed in “Procedures when reinstalling the LDAP server” on page 20.

Attention:

- Before committing to the conversion of a large LDAP database, customers should experiment with the data conversion procedure on a set of test systems.
- Before attempting the data conversion procedure in a production environment, customers should backup the LDAP database using the recommended tools for that LDAP product.

Procedures when not reinstalling the LDAP server

If you are not reinstalling the LDAP server as part of the conversion process, use the procedure that is appropriate for your LDAP server.

IBM Tivoli Directory Server procedure

If you are converting the data and do not need to reinstall the LDAP server, perform the following steps:

1. Stop all Tivoli Access Manager servers and blade products.
2. From this point onward in the data conversion procedure, additions or modifications to Tivoli Access Manager users, groups, or policy definitions, such as those performed with the **pdadmin** utility, must be halted until after the completion of the data conversion procedure.
3. Export the LDAP database to an LDIF file and save the file. This file will be the input LDIF file to the **amldif2v6** tool.
 - a. Using the IBM Tivoli Directory Server Configuration Tool, select **Export LDIF data**.
 - b. Type the name of a new file into which you want to export your LDAP data.
 - c. Leave the **subtree DN** field blank.
 - d. Click **Export**.
 - e. Save the LDIF file. Keep it secure, because it contains the contents of the LDAP database.
4. Use the Tivoli Access Manager **pdbackup** command to back up all Tivoli Access Manager data. The usage of this command is described in the *IBM Tivoli Access Manager for e-business: Command Reference*. This step is only a precautionary measure.
5. Use the instructions in the *IBM Tivoli Access Manager for e-business: Upgrade Guide* to upgrade your Tivoli Access Manager enterprise.
6. Ensure that the LDAP server is up and running.
7. Run the **ivrgy_tool** utility to update the LDAP schema definitions with the schema updates required by Tivoli Access Manager 6.0. The syntax of this utility is as follows:


```
ivrgy_tool -h ldap_server_name -p port number -D ldap_server_admin_dn -w ldap_admin_password -d schema
```

The usage of this command is described in the *IBM Tivoli Access Manager for e-business: Command Reference*.
8. Stop and restart the LDAP server.
9. Restart all Tivoli Access Manager servers and blade products.
10. Verify the functionality of Tivoli Access Manager using the **pdadmin** utility to display a few configured users and groups.

At this point, your Tivoli Access Manager enterprise is upgraded to version 6.0. However, this enterprise has yet to take advantage of the new LDAP data model.

11. Use the **amldif2v6** utility and the input LDIF file produced in step 3 to generate an LDIF representation of the LDAP database. This representation contains the modifications to the Tivoli Access Manager LDAP data that are required by the new LDAP data model. The syntax of the **amldif2v6** utility is described in “amldif2v6 syntax” on page 6. For details about what is happening, see “The data-conversion processes” on page 30.
12. Stop all Tivoli Access Manager servers and blade products.
13. Delete all of the user-defined objects from the LDAP database.
 - a. Stop the IBM Tivoli Directory Server.
 - b. Unconfigure the database:
 - 1) Using the IBM Tivoli Directory Server Configuration Tool, select the **Unconfigure database** option.
 - 2) Select **Unconfigure and destroy database**.
 - 3) Click the **Unconfigure** button.
 - 4) Click the **OK** button to unconfigure the database.
 - c. Create the new database:
 - 1) Using the IBM Tivoli Directory Server Configuration Tool, select the **Configure database** option.
 - 2) Select **Create new database**.
 - 3) Click the **Next** button.
 - 4) Enter a valid user name and password.
 - 5) Click the **Next** button.
 - 6) Enter a name for the new database.
 - 7) Click the **Next** button.
 - 8) Select a character set for the new database.
 - 9) Click the **Next** button.
 - 10) Select the database location.
 - 11) Click the **Next** button.
 - 12) Click the **Finish** button.

Several alternative methods for this step are described in “Deleting LDAP objects before importing the output file” on page 10.

14. Import the entire contents of the output LDIF file that was created in step 11. If importing an LDIF file which contains 10000 users or less, use the **ldapadd** command to import the file. Otherwise, follow the instructions in the *Tivoli Access Manager: Performance Tuning Guide* for importing large LDIF files using the **bulkload** command.

The syntax of the **ldapadd** command is as follows:

```
ldapadd -h ldapServerHostName -D ldapAdminDN -w ldapAdminPassword -p
ldapPortNumber -f ldifFilename
```

- a. Follow the instructions for the appropriate command to import the data.
- b. Restart the LDAP server.
15. Restart all Tivoli Access Manager servers and blade products.
16. Verify the functionality of Tivoli Access Manager using the **pdadmin** utility to display a few configured users and groups.

The data conversion procedure is complete.

Sun Java System Directory Server procedure

If you are converting the data and do not need to reinstall the LDAP server, perform the following steps:

1. Stop all Tivoli Access Manager servers and blade products.
2. From this point onward in the data conversion procedure, additions or modifications to Tivoli Access Manager users, groups, or policy definitions, such as those performed with the **pdadmin** utility, must be halted until after the completion of the data conversion procedure.
3. Export the LDAP database to an LDIF file and save the file. This file will be the input LDIF file to the **amldif2v6** tool.
 - a. Using the Sun Directory Server Console, expand the object tree on the left and double click **Directory Server**.
 - b. Select the **Tasks** tab.
 - c. Click **Log into Directory Server as new user** and log in as cn=Directory Manager.
 - d. Click **Export databases**.
 - e. Type the name of a new file into which you want to export your LDAP data.
 - f. Ensure that the **All databases** option is selected.
 - g. Click **OK** to export the data to the specified file.
 - h. When the export completes, click **Close**.
 - i. Save the LDIF file. Keep it secure, because it contains the contents of the LDAP database.
4. Use the Tivoli Access Manager **pdbackup** command to back up all Tivoli Access Manager data. The usage of this command is described in the *IBM Tivoli Access Manager for e-business: Command Reference*. This step is only a precautionary measure.
5. Use the instructions in the *IBM Tivoli Access Manager for e-business: Upgrade Guide* to upgrade your Tivoli Access Manager enterprise.
6. Ensure that the LDAP server is up and running.
7. Run the **ivrgy_tool** utility to update the LDAP schema definitions with the schema updates required by Tivoli Access Manager 6.0. The syntax of this utility is as follows:


```
ivrgy_tool -h ldap_server_name -p port number -D ldap_server_admin_dn -w ldap_admin_password -d schema
```

The usage of this command is described in the *IBM Tivoli Access Manager for e-business: Command Reference*.
8. Stop and restart the LDAP server.
9. Restart all Tivoli Access Manager servers and blade products.
10. Verify the functionality of Tivoli Access Manager using the **pdadmin** utility to display a few configured users and groups.

At this point, your Tivoli Access Manager enterprise is upgraded to version 6.0. However, this enterprise has yet to take advantage of the new LDAP data model.
11. Use the **amldif2v6** utility and the input LDIF file produced in step 3 to generate an LDIF representation of the LDAP database. This representation contains the modifications to the Tivoli Access Manager LDAP data that are required by the new LDAP data model. The syntax of the **amldif2v6** utility is

described in “amldif2v6 syntax” on page 6. For details about what is happening, see “The data-conversion processes” on page 30.

12. Stop all Tivoli Access Manager servers and blade products.
13. Delete all of the user-defined objects from the LDAP database using the following procedure to delete and recreate their associated databases:
 - a. Using the Sun Directory Server Console, select the **Configuration** tab.
 - b. Click on the + to expand **Data**.
 - c. For each suffix displayed, except cn=NetscapeRoot, do the following:
 - 1) Click the + of each suffix to display its associated database.
 - 2) Left click the database to select it.
 - 3) Right click the database.
 - 4) Click **Delete**.
 - 5) Click **Yes** to delete the database.

Note: Do not delete the database that is associated with the cn=NetscapeRoot suffix. Deleting this database damages the functionality of the Sun Java System Directory Server. It is assumed that there are no Tivoli Access Manager users or groups defined beneath this suffix. If this assumption is false, all user-defined user and group objects that were created beneath this suffix must be manually deleted.

- d. Left click the suffix to select it.
- e. Right click the suffix.
- f. Click **New Database**.
- g. Type a unique database name and click **OK**.
- h. Click **YES** to enable the suffix for which the database is being created.
- i. Select the **Tasks** tab.
- j. Restart the LDAP server.

Several alternative methods for how this might be accomplished are described in “Deleting LDAP objects before importing the output file” on page 10.

14. Import the entire contents of the output LDIF file that was created in step 11.
 - a. Using the Sun Directory Server Console, click the **Tasks** tab.
 - b. Select **Import databases**.
 - c. For the name of the LDIF file, type the name of the LDIF file that was generated by the **amldif2v6** utility in step 11.
 - d. Ensure that the **Continue on error** box is selected.
 - e. Type a file name in the **file for rejects** field.
 - f. Click **OK** to begin the import operation.

A number of object already exists errors will be logged during the import operation. These errors should be associated with objects under the o=NetscapeRoot suffix, which the LDIF file attempted to recreate. These errors can be ignored. These should be the only errors reported.
15. Restart all Tivoli Access Manager servers and blade products.
16. Verify the functionality of Tivoli Access Manager using the **pdadmin** utility to display a few configured users and groups.

The data conversion procedure is complete.

Novell eDirectory procedure

If you are converting the data and do not need to reinstall the LDAP server, perform the following steps:

1. Stop all Tivoli Access Manager servers and blade products.
2. From this point onward in the data conversion procedure, additions or modifications to Tivoli Access Manager users, groups, or policy definitions, such as those performed with the **pdadmin** utility, must be halted until after the completion of the data conversion procedure.
3. For Novell eDirectory, you cannot use native tools to export the LDAP database. To export only that portion of the LDAP database directly affected by the data model change, use the **getamobjects** utility.
 - If working on Windows®, obtain a copy of the Tivoli Access Manager **getamobjects.bat** utility.
 - If working on Linux® or UNIX®, obtain a copy of the Tivoli Access Manager **getamobjects.sh** utility.

The **getamobjects** utility enable you to export the Tivoli Access Manager LDAP objects that are affected by the data model change. However, before you can run this utility, you must edit it. Follow the instructions in the file for editing its content.

Run the updated **getamobjects** utility. The Tivoli Access Manager LDAP objects will be saved to the `inputLDIFfile` LDIF file that is located in the current directory. This file will be the input LDIF file for the **amldif2v6** utility.

4. Use the Tivoli Access Manager **pdbackup** command to back up all Tivoli Access Manager data. The usage of this command is described in the *IBM Tivoli Access Manager for e-business: Command Reference*. This step is only a precautionary measure.
5. Use the instructions in the *IBM Tivoli Access Manager for e-business: Upgrade Guide* to upgrade your Tivoli Access Manager enterprise.
6. Ensure that the LDAP server is up and running.
7. Run the **ivrgy_tool** utility to update the LDAP schema definitions with the schema updates required by Tivoli Access Manager 6.0. The syntax of this utility is as follows:

```
ivrgy_tool -h ldap_server_name -p port number -D ldap_server_admin_dn
-w ldap_admin_password -d schema
```

The usage of this command is described in the *IBM Tivoli Access Manager for e-business: Command Reference*.

8. Stop and restart the LDAP server.
9. Restart all Tivoli Access Manager servers and blade products.
10. Verify the functionality of Tivoli Access Manager using the **pdadmin** utility to display a few configured users and groups.

At this point, your Tivoli Access Manager enterprise is upgraded to version 6.0. However, this enterprise has yet to take advantage of the new LDAP data model.
11. Use the **amldif2v6** utility and the input LDIF file produced in step 3 to generate an LDIF representation of the LDAP database. This representation contains the modifications to the Tivoli Access Manager LDAP data that are required by the new LDAP data model. The syntax of the **amldif2v6** utility is described in “amldif2v6 syntax” on page 6. For details about what is happening, see “The data-conversion processes” on page 30.
12. Stop all Tivoli Access Manager servers and blade products.

13. Delete all of the user-defined objects from the LDAP database.
 - If working on Windows, obtain a copy of the Tivoli Access Manager **deleteamobjects.bat** utility.
 - If working on Linux or UNIX, obtain a copy of the Tivoli Access Manager **deleteamobjects.sh** utility.

The **deleteamobjects** utility enables you to selectively delete the Tivoli Access Manager LDAP objects from the Novell eDirectory database that are associated with the old data model. The **deleteamobjects** utility must be edited before use. Follow the instructions in the file for editing its contents.

Run the updated **deleteamobjects** utility.

14. Import the entire contents of the output LDIF file that was created in step 11.
 - a. Edit *all* secAuthorityInfo objects found in the file that was generated by the **amldif2v6** utility in step 11 as follows:
 - 1) Retain the line which specifies the dn: of the secAuthorityInfo object. Do not modify it.
 - 2) Beneath the line which specifies the dn: of the secAuthorityInfo object, add a line which contains the text changetype: modify.
 - 3) Beneath the changetype: modify line, add a line which contains the text replace: Version.
 - 4) Beneath the replace: Version line, add a line which contains the text Version: 6.0.
 - 5) Delete all of the other lines contained within the definition of the secAuthorityInfo object.

The secAuthority: default object within this file will now appear as follows:

```
dn: secAuthority=Default
changetype: modify
replace: Version
Version: 6.0
```

- b. Edit each secAuthorityInfo object found within this file in the same fashion. If migrating from Tivoli Access Manager 4.1 to Tivoli Access Manager 6.0, also add an LDIF entry that adds an installDate attribute to each secAuthorityInfo object. The following example is for the secAuthority=Default object:


```
dn: secAuthority=Default
changetype: modify
add: installDate
installDate: 20051025051350.0Z
```
- c. Start the Novell eDirectory ConsoleOne utility.
- d. Click the **Wizards** pull down and select **NDS Import/Export**.
- e. Select **Import LDIF Files**.
- f. Click **Advanced**.
- g. Type a name for the **LDIF Output File for Failed Records**.
- h. Select **Run in verbose mode**.
- i. Click **OK**.
- j. Click **Next**.
- k. Type the name of the source LDIF file (that is, the input LDIF file produced by the **amldif2v6** utility in step 11).
- l. Click **Next**.

- m. Type the server DNS name (or the IP address) of the Novell eDirectory server and the port number on which it is listening, select **Authenticated login**, and type the DN of the Novell eDirectory administrator and password.
 - n. Click **Next**.
 - o. Click **Finish** to import the file.
- Examine the Output File for Failed Records to learn whether errors were experienced during the import operation.
- 15. Restart all Tivoli Access Manager servers and blade products.
 - 16. Verify the functionality of Tivoli Access Manager using the **pdadmin** utility to display a few configured users and groups.

The data conversion procedure is complete.

Procedures when reinstalling the LDAP server

If you are reinstalling the LDAP server as part of the conversion process, use the procedure that is appropriate for you LDAP server.

IBM Tivoli Directory Server procedure

If you are converting the data and plan to reinstall the LDAP server, perform the following steps:

1. Stop all Tivoli Access Manager servers and blade products.
2. From this point onward in the data conversion procedure, additions or modifications to Tivoli Access Manager users, groups, or policy definitions, such as those performed with the **pdadmin** utility, must be halted until after the completion of the data conversion procedure.
3. Export the LDAP database to an LDIF file and save the file. This file will be the input LDIF file to the **amldif2v6** tool.
 - a. Using the IBM Tivoli Directory Server Configuration Tool, select **Export LDIF data**.
 - b. Type the name of a new file into which you want to export your LDAP data.
 - c. Leave the **subtree DN** field blank.
 - d. Click **Export**.
 - e. Save the LDIF file. Keep it secure, because it contains the contents of the LDAP database.
4. Use the Tivoli Access Manager **pdbackup** command to back up all Tivoli Access Manager data. The usage of this command is described in the *IBM Tivoli Access Manager for e-business: Command Reference*. This step is only a precautionary measure.
5. Reinstall the LDAP server with a version that is compatible with Tivoli Access Manager, version 6.0.
6. Use the instructions in the *IBM Tivoli Access Manager for e-business: Upgrade Guide* to upgrade your Tivoli Access Manager enterprise. Take care not to start any of the Tivoli Access Manager daemons, because the LDAP server was reinstalled with a newer version.
7. Ensure that the LDAP server is up and running.
8. Run the **ivrgy_tool** utility to update the LDAP schema definitions with the schema updates required by Tivoli Access Manager 6.0. The syntax of this utility is as follows:

```
ivrgy_tool -h ldap_server_name -p port number -D ldap_server_admin_dn
-w ldap_admin_password -d schema
```

The usage of this command is described in the *IBM Tivoli Access Manager for e-business: Command Reference*.

9. Stop and restart the LDAP server.
10. Recreate, but do not instantiate, all suffixes that previously existed on the previous LDAP server before the data that was backed up earlier can be re-imported.
 - a. Create, but do not instantiate, these suffixes now using the administration tools that come with the LDAP server.
 - b. Stop and restart the LDAP server.
11. Use the **amldif2v6** utility and the input LDIF file produced in step 3 to generate an LDIF representation of the LDAP database. This representation contains the modifications to the Tivoli Access Manager LDAP data that are required by the new LDAP data model. The syntax of the **amldif2v6** utility is described in “amldif2v6 syntax” on page 6. For details about what is happening, see “The data-conversion processes” on page 30.
12. Import the entire contents of the output LDIF file that was created in step 11. If importing an LDIF file which contains 10000 users or less, use the **ldapadd** command to import the file. Otherwise, follow the instructions in the *Tivoli Access Manager: Performance Tuning Guide* for importing large LDIF files using the **bulkload** command.
The syntax of the **ldapadd** command is as follows:

```
ldapadd -h ldapServerHostName -D ldapAdminDN -w ldapAdminPassword -p
ldapPortNumber -f ldifFilename
```

 - a. Follow the instructions for the appropriate command to import the data.
 - b. Restart the LDAP server.
13. Restart all Tivoli Access Manager servers and blade products.
14. Verify the functionality of Tivoli Access Manager using the **pdadmin** utility to display a few configured users and groups.

The data conversion procedure is now complete.

Sun Java System Directory Server procedure

If you are converting the data and plan to reinstall the LDAP server, perform the following steps:

1. Stop all Tivoli Access Manager servers and blade products.
2. From this point onward in the data conversion procedure, additions or modifications to Tivoli Access Manager users, groups, or policy definitions, such as those performed with the **pdadmin** utility, must be halted until after the completion of the data conversion procedure.
3. Export the LDAP database to an LDIF file and save the file. This file will be the input LDIF file to the **amldif2v6** tool.
 - a. Using the Sun Directory Server Console, expand the object tree on the left and double click **Directory Server**.
 - b. Select the **Tasks** tab.
 - c. Click **Log into Directory Server as new user** and log in as cn=Directory Manager.
 - d. Click **Export databases**.

- e. Type the name of a new file into which you want to export your LDAP data.
 - f. Ensure that the **All databases** option is selected.
 - g. Click **OK** to export the data to the specified file.
 - h. When the export completes, click **Close**.
 - i. Save the LDIF file. Keep it secure, because it contains the contents of the LDAP database.
4. Use the Tivoli Access Manager **pdbbackup** command to back up all Tivoli Access Manager data. The usage of this command is described in the *IBM Tivoli Access Manager for e-business: Command Reference*. This step is only a precautionary measure.
 5. Reinstall the LDAP server with a version that is compatible with Tivoli Access Manager, version 6.0.
 6. Use the instructions in the *IBM Tivoli Access Manager for e-business: Upgrade Guide* to upgrade your Tivoli Access Manager enterprise. Take care not to start any of the Tivoli Access Manager daemons, because the LDAP server was reinstalled with a newer version.
 7. Ensure that the LDAP server is up and running.
 8. Run the **ivrgy_tool** utility to update the LDAP schema definitions with the schema updates required by Tivoli Access Manager 6.0. The syntax of this utility is as follows:


```
ivrgy_tool -h ldap_server_name -p port number -D ldap_server_admin_dn
-w ldap_admin_password -d schema
```

The usage of this command is described in the *IBM Tivoli Access Manager for e-business: Command Reference*.
 9. Stop and restart the LDAP server.
 10. Recreate, but do not instantiate, all suffixes that previously existed on the previous LDAP server before the data that was backed up earlier can be re-imported.
 - a. Create, but do not instantiate, these suffixes now using the administration tools that come with the LDAP server.
 - b. Stop and restart the LDAP server.
 11. Use the **amldif2v6** utility and the input LDIF file produced in step 3 to generate an LDIF representation of the LDAP database. This representation contains the modifications to the Tivoli Access Manager LDAP data that are required by the new LDAP data model. The syntax of the **amldif2v6** utility is described in “amldif2v6 syntax” on page 6. For details about what is happening, see “The data-conversion processes” on page 30.
 12. Import the entire contents of the output LDIF file that was created in step 11.
 - a. Using the Sun Directory Server Console, click the **Tasks** tab.
 - b. Select **Import databases**.
 - c. For the name of the LDIF file, type the name of the LDIF file that was generated by the **amldif2v6** utility in step 11.
 - d. Ensure that the **Continue on error** box is selected.
 - e. Type a file name in the **file for rejects** field.
 - f. Click **OK** to begin the import operation.

A number of object already exists errors will be logged during the import operation. These errors should be associated with objects under the o=NetscapeRoot suffix, which the LDIF file attempted to recreate. These errors can be ignored. These should be the only errors reported.

13. Restart all Tivoli Access Manager servers and blade products.
14. Verify the functionality of Tivoli Access Manager using the **pdadmin** utility to display a few configured users and groups.

The data conversion procedure is now complete.

Novell eDirectory procedure

If you are converting the data and plan to reinstall the LDAP server, perform the following steps:

1. Stop all Tivoli Access Manager servers and blade products.
2. From this point onward in the data conversion procedure, additions or modifications to Tivoli Access Manager users, groups, or policy definitions, such as those performed with the **pdadmin** utility, must be halted until after the completion of the data conversion procedure.
3. For Novell eDirectory, you cannot use native tools to export the LDAP database. To export only that portion of the LDAP database directly affected by the data model change, use the **getamobjects** utility.
 - If working on Windows, obtain a copy of the Tivoli Access Manager **getamobjects.bat** utility.
 - If working on Linux or UNIX, obtain a copy of the Tivoli Access Manager **getamobjects.sh** utility.

The **getamobjects** utility enable you to export the Tivoli Access Manager LDAP objects that are affected by the data model change. However, before you can run this utility, you must edit it. Follow the instructions in the file for editing its content.

Run the updated **getamobjects** utility. The Tivoli Access Manager LDAP objects will be saved to the inputLDIFfile LDIF file that is located in the current directory. This file will be the input LDIF file for the **amldif2v6** utility.

4. Use the Tivoli Access Manager **pdbackup** command to back up all Tivoli Access Manager data. The usage of this command is described in the *IBM Tivoli Access Manager for e-business: Command Reference*. This step is only a precautionary measure.
5. Reinstall the LDAP server with a version that is compatible with Tivoli Access Manager, version 6.0.
6. Use the instructions in the *IBM Tivoli Access Manager for e-business: Upgrade Guide* to upgrade your Tivoli Access Manager enterprise. Take care not to start any of the Tivoli Access Manager daemons, because the LDAP server was reinstalled with a newer version.
7. Ensure that the LDAP server is up and running.
8. Run the **ivrgy_tool** utility to update the LDAP schema definitions with the schema updates required by Tivoli Access Manager 6.0. The syntax of this utility is as follows:

```
ivrgy_tool -h ldap_server_name -p port number -D ldap_server_admin_dn
-w ldap_admin_password -d schema
```

The usage of this command is described in the *IBM Tivoli Access Manager for e-business: Command Reference*.

9. Stop and restart the LDAP server.
10. Use the **amldif2v6** utility and the input LDIF file produced in step 3 to generate an LDIF representation of the LDAP database. This representation contains the modifications to the Tivoli Access Manager LDAP data that are required by the new LDAP data model. The syntax of the **amldif2v6** utility is

described in “amldif2v6 syntax” on page 6. For details about what is happening, see “The data-conversion processes” on page 30.

11. Import the entire contents of the output LDIF file that was created in step 10.
 - a. Edit *all* secAuthorityInfo objects found in the file that was generated by the **amldif2v6** utility in step 10 as follows:
 - 1) Retain the line which specifies the dn: of the secAuthorityInfo object. Do not modify it.
 - 2) Beneath the line which specifies the dn: of the secAuthorityInfo object, add a line which contains the text changetype: modify.
 - 3) Beneath the changetype: modify line, add a line which contains the text replace: Version.
 - 4) Beneath the replace: Version line, add a line which contains the text Version: 6.0.
 - 5) Delete all of the other lines contained within the definition of the secAuthorityInfo object.

The secAuthority: default object within this file will now appear as follows:

```
dn: secAuthority=Default
changetype: modify
replace: Version
Version: 6.0
```

- b. Edit each secAuthorityInfo object found within this file in the same fashion. If migrating from Tivoli Access Manager 4.1 to Tivoli Access Manager 6.0, also add an LDIF entry that adds an installDate attribute to each secAuthorityInfo object. The following example is for the secAuthority=Default object:

```
dn: secAuthority=Default
changetype: modify
add: installDate
installDate: 20051025051350.0Z
```

- c. Start the Novell eDirectory ConsoleOne utility.
- d. Click the **Wizards** pull down and select **NDS Import/Export**.
- e. Select **Import LDIF Files**.
- f. Click **Advanced**.
- g. Type a name for the **LDIF Output File for Failed Records**.
- h. Select **Run in verbose mode**.
- i. Click **OK**.
- j. Click **Next**.
- k. Type the name of the source LDIF file (that is, the input LDIF file produced by the **amldif2v6** utility in step 10).
- l. Click **Next**.
- m. Type the server DNS name (or the IP address) of the Novell eDirectory server and the port number on which it is listening, select **Authenticated login**, and type the DN of the Novell eDirectory administrator and password.
- n. Click **Next**.
- o. Click **Finish** to import the file.

Examine the Output File for Failed Records to learn whether errors were experienced during the import operation.

12. Restart all Tivoli Access Manager servers and blade products.

13. Verify the functionality of Tivoli Access Manager using the **pdadmin** utility to display a few configured users and groups.

The data conversion procedure is now complete.

Chapter 6. Installation

The **amldif2v6** data model conversion utility is available from the IBM Tivoli Access Manager for e-business Software Support Web site at the following Web address:

<http://www.ibm.com/software/sysmgmt/products/support/IBMTivoliAccessManagerfore-business.html>

After the customer decides to convert the data to the new data model and downloads this utility, it should be copied to the following location on the local Tivoli Access Manager system:

Linux or UNIX

`/opt/PolicyDirector/sbin`

Windows

`install_base\sbin`

By default, *install_base* is `c:\Program Files\Tivoli\PolicyDirector`

If using Novell eDirectory, the tools **getamobjects** and **deleteamobjects** should be copied to the same location as **amldif2v6** on the local Tivoli Access Manager system.

Chapter 7. Performance

This section provides information about the overall performance of the conversion process and details about improving the performance of the **amldif2v6** utility.

Overall performance

If a customer chooses to convert an existing Tivoli Access Manager configuration to use the new data model, the overall performance of the conversion process depends on the following criteria:

- The size of the customer environment
- The performance of the native LDAP tools that are available for exporting the existing data into LDIF format
- The time it takes to run the conversion tool to create the new LDIF to be reloaded
- The performance of the native LDAP tools that are available to import the new LDIF into the LDAP database

Tools, such as the IBM Tivoli Directory Server **bulkload** utility that have the ability to load an LDIF data file directly into the LDAP database, usually perform better than tools, such as the **ldif2db** utility that often loads the LDIF data by going through LDAP protocols to the LDAP server.

Customers are strongly encouraged to experiment ahead of time with the performance of these tools and the conversion process before committing themselves to the conversion of extremely large LDAP user registries.

Improving conversion tool-specific performance

The **amldif2v6** utility accepts input parameters for the *maximum* number of entries for its *in-memory user cache* and for the *maximum* number of entries for its *in-memory group cache*. The size of the user cache will typically have a greater impact on the performance of the **amldif2v6** utility, because the number of Tivoli Access Manager users in an LDAP database usually exceeds the number of Tivoli Access Manager groups in an LDAP database.

The **amldif2v6** utility iteratively copies user-related data objects and group-related data objects from the input LDIF file to the “in-memory user object cache” and to the “in-memory group object cache”, respectively. The tools copies these data objects until either of the in-memory caches is full or until the utility reaches the end of the input LDIF file. In both of these situations, the **amldif2v6** utility performs the data conversion on the data in the caches and writes the converted data to the output LDIF file.

To achieve acceptable performance for large input LDIF files, the customer will want to run the **amldif2v6** utility on a fast machine with as much physical memory as possible. The **amldif2v6** utility needs to read the input LDIF file the following number of times, whichever number is larger:

- The number of Tivoli Access Manager user-related data objects in the input LDIF file divided by the number of entries defined for the in-memory user cache parameter

- The number of Tivoli Access Manager group-related data objects in the input LDIF file divided by the number of entries defined for the in-memory group cache parameter

Typically, the number of Tivoli Access Manager groups in the input LDIF file is small when compared to the number of Tivoli Access Manager users. Therefore, a larger in-memory user cache usually enables the utility to process more entries on each read iteration of the input LDIF file. Customers who are processing large LDIF files will typically want to make the size of the in-memory user cache as large as possible.

Determining the size of the in-memory user cache

The **amldif2v6** utility allocates a little more than 4 MB of memory for each 1000 entries plus the size of its in-memory user cache. If the user cache size is made too large, which might cause the physical memory to be overcommitted, the **amldif2v6** utility will cause the operating system to begin swapping. If swapping occurs, the performance of the **amldif2v6** utility will degrade significantly. Customers should experiment with a relatively small input LDIF file (around 200,000 users) to tune the size of the user cache to the size of physical memory before attempting to process very large input LDIF files.

Begin tuning the **amldif2v6** utility with the following values for the size of the in-memory user cache and the in-memory group cache.

```
amldif2v6 input_ldif_filename output_ldif_filename 5000 300
```

If the performance of these settings is unacceptable and you have not overcommitted physical memory, try increasing the value of the in-memory user cache. Conversely, the performance of these settings might be unacceptable, because you overcommitted physical memory. Try reducing the cache settings to acceptable values. The sizes of the caches have no limits other than the constraint imposed by the amount of available physical memory.

The data-conversion processes

The input file for the **amldif2v6** utility is the file that contains the LDIF representation of the customer's entire LDAP database. The **amldif2v6** utility performs the following processes:

1. Copies the input LDIF file to a temporary file that the utility can modify. From this point onward, the original input LDIF file is not touched. The original input LDIF file is never modified.
2. Moves all of the objects from the temporary input LDIF file that are not involved in the data model conversion process to the output LDIF file. During this process, all LDAP objects that were not created by Tivoli Access Manager are moved to the output LDIF file.
3. Reads Tivoli Access Manager user-related and group-related data objects from the temporary input LDIF file into the in-memory user object cache and the in-memory group object cache, respectively, until either both caches are full or until there are no more data objects to read in the temporary input file.
4. Converts the entries in the caches and writes them to the output LDIF file.
5. Repeats step 3 until there are no more entries to read in the temporary input file.
6. The program exits after writing the last converted entry to the output LDIF file.

Notices

This information was developed for products and services offered in the U.S.A. IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

For license inquiries regarding double-byte (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

IBM World Trade Asia Corporation
Licensing
2-31 Roppongi 3-chome, Minato-ku
Tokyo 106, Japan

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law:

INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement 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 78758
U.S.A.

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement or any equivalent agreement between us.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

All statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

If you are viewing this information softcopy, the photographs and color illustrations may not appear.

Trademarks

IBM, IBM logo, DB2, Tivoli, and Tivoli logo are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both.

Java and all Java-based trademarks and logos are trademarks or registered trademarks of Sun Microsystems, Inc. in the United States and other countries.

Linux is a 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.

Other company, product, or service names may be trademarks or service marks of others.



IBM Confidential
Printed in USA