Informatica

Informatica® Dynamic Data Masking
9.9

Active Directory Accelerator Guide

Informatica Dynamic Data Masking Active Directory Accelerator Guide
9.9
February 2019

Revision: 1
Publication Date: 2019-02-18

Table of Contents

Preface

The *Active Directory Accelerator Guide* contains information to help administrators use the Active Directory accelerator to implement Dynamic Data Masking for an LDAP directory. This guide assumes that you have knowledge of Dynamic Data Masking.

Informatica Resources

Informatica provides you with a range of product resources through the Informatica Network and other online portals. Use the resources to get the most from your Informatica products and solutions and to learn from other Informatica users and subject matter experts.

Informatica Network

The Informatica Network is the gateway to many resources, including the Informatica Knowledge Base and Informatica Global Customer Support. To enter the Informatica Network, visit https://network.informatica.com.

As an Informatica Network member, you have the following options:

- Search the Knowledge Base for product resources.
- View product availability information.
- Create and review your support cases.
- Find your local Informatica User Group Network and collaborate with your peers.

Informatica Knowledge Base

Use the Informatica Knowledge Base to find product resources such as how-to articles, best practices, video tutorials, and answers to frequently asked questions.

To search the Knowledge Base, visit https://search.informatica.com. If you have questions, comments, or ideas about the Knowledge Base, contact the Informatica Knowledge Base team at KB_Feedback@informatica.com.

Informatica Documentation

Use the Informatica Documentation Portal to explore an extensive library of documentation for current and recent product releases. To explore the Documentation Portal, visit https://docs.informatica.com.

Informatica maintains documentation for many products on the Informatica Knowledge Base in addition to the Documentation Portal. If you cannot find documentation for your product or product version on the Documentation Portal, search the Knowledge Base at https://search.informatica.com.

If you have questions, comments, or ideas about the product documentation, contact the Informatica Documentation team at infa_documentation@informatica.com.

Informatica Product Availability Matrices

Product Availability Matrices (PAMs) indicate the versions of the operating systems, databases, and types of data sources and targets that a product release supports. You can browse the Informatica PAMs at https://network.informatica.com/community/informatica-network/product-availability-matrices.

Informatica Velocity

Informatica Velocity is a collection of tips and best practices developed by Informatica Professional Services and based on real-world experiences from hundreds of data management projects. Informatica Velocity represents the collective knowledge of Informatica consultants who work with organizations around the world to plan, develop, deploy, and maintain successful data management solutions.

You can find Informatica Velocity resources at http://velocity.informatica.com. If you have questions, comments, or ideas about Informatica Velocity, contact Informatica Professional Services at ips@informatica.com.

Informatica Marketplace

The Informatica Marketplace is a forum where you can find solutions that extend and enhance your Informatica implementations. Leverage any of the hundreds of solutions from Informatica developers and partners on the Marketplace to improve your productivity and speed up time to implementation on your projects. You can find the Informatica Marketplace at https://marketplace.informatica.com.

Informatica Global Customer Support

You can contact a Global Support Center by telephone or through the Informatica Network.

To find your local Informatica Global Customer Support telephone number, visit the Informatica website at the following link:
https://www.informatica.com/services-and-training/customer-success-services/contact-us.html.

To find online support resources on the Informatica Network, visit https://network.informatica.com and select the eSupport option.

CHAPTER 1

Introduction to the Active Directory Accelerator

This chapter includes the following topic:

Active Directory Accelerator Overview

Use the Active Directory accelerator to implement Dynamic Data Masking for an LDAP directory. The accelerator package contains predefined Dynamic Data Masking security rules for common masking requirements.

The Active Directory accelerator is in the Dynamic Data Masking installation folder as an additional component that you can configure to work with an LDAP directory. You can use the accelerator rules to mask data based on lists of authorized and unauthorized users, groups, and attributes.

CHAPTER 2

Active Directory Accelerator Setup

This chapter includes the following topics:

Active Directory Accelerator Setup Overview

Set up the Active Directory accelerator to use predefined connection and security rules.

You can find the Active Directory accelerator in the following directory:

```
<Dynamic Data Masking installation>\Accelerators\ActiveDirectory
```

To set up the Active Directory accelerator, perform the following tasks:

1. Verify the setup requirements.
2. Configure the Active Directory Accelerator.
3. Create a Dynamic Data Masking database connection.
4. Create a connection rule.
5. Import the Active Directory accelerator security rules.

Verify Requirements

Verify the following requirements before you use the Active Directory accelerator:

- You must have Dynamic Data Masking version 9.1.0 or later installed.
- You must have a database with an LDAP directory.

Configure the Active Directory Accelerator

To configure the Active Directory accelerator, define the parameters in the ldap.properties file.

You can find the sample_ldap.properties file in the following directory:

```
<Dynamic Data Masking installation>\Accelerators\ActiveDirectory\cfg
```

After you edit the file, you must save it as ldap.properties in the following directory:

```
<Dynamic Data Masking installation>\custom\cfg\ldap.properties
```

For UNIX and Linux, save ldap.properties in the following directory:

```
<Dynamic Data Masking installation>/custom/cfg/ldap.properties
```

The following table describes the parameters that you define in the sample_ldap.properties file:

Parameter	Description
hostname	The host name or IP address of the LDAP directory.
port	The LDAP port. Default is 389.
authentication	The LDAP authentication. The authentication can be simple or none.
basedn	The domain name in the LDAP directory format. For example, if the domain name is mycompany.com, enter the following text: `basedn=DC\=mycompany,DC\=com`
principal	The user name that connects to the LDAP directory followed by @<domain name>, such as jsmith@mycompany.com. Required if you configure the authentication to be simple.
rootpwd	The password of the user that connects to the LDAP directory. Required if you configure the authentication to be simple. After you start the Active Directory accelerator the first time, the rootpwd value is encrypted and the passwordEncrypted property is set to true.

Create a Database Connection

Create a Dynamic Data Masking database connection in the Management Console.

1. Log in to the Dynamic Data Masking Management Console.
2. Select the Dynamic Data Masking Server in the Management Console tree and click **Tree** > **Add DDM Services**.

   The **Add DDM Services** window appears.
3. Select the service that you want to add and click **OK.**

   The Dynamic Data Masking service node appears in the Management Console tree.
4. Select a domain node or the Management Console tree root node and click **Tree** > **Add Database**.

   The **Add Database** window appears.
5. Select the database type and configure the database connection parameters.

6. Click **Test Connection** and verify that Dynamic Data Masking is connected to the database.
7. Click **OK**.

   The database node appears in the Management Console.

Create a Connection Rule

Create a connection rule that directs SQL requests to the LDAP Rule Set.

1. Select the Dynamic Data Masking service node that you created in the Management Console tree and click **Tree** > **Connection Rules**.

   The **Rule Editor** opens.
2. In the **Rule Editor**, highlight the Dynamic Data Masking service node in the tree and select **Action** > **Append Rule**.

   The **Append Rule** window opens.
3. In the **Append Rule** window, configure the following parameters:

Parameter	Description
Rule Name	The name of the connection rule.
Identify incoming connections using	Select Current Target Database.
Database	The name of the database.
Action applied on incoming connections	Select Use Rule Set.
Rule Set Name	Define the rule set name as LDAP Rule Set.
Whenever this rule is matched	Select stop if applied.

4. Click **OK**.

   The rule appears in the **Rule Editor**.
5. Select **File** > **Update Rules** to save the connection rule.
6. Select **File** > **Exit** to close the **Rule Editor**.

Import the Security Rules

Import the predefined Active Directory accelerator security rules into the Management Console.

1. Select the Management Console tree root node and click **Tree** > **Security Rule Set**.

   The **Add Rule Set** window opens.
2. Enter "LDAP Rule Set" as the rule set name and click **OK**.

   The LDAP Rule Set node appears in the Management Console tree.

3. Select the LDAP Rule Set rule set and click **Tree** > **Security Rule Set**.

   The **Rule Editor** opens.

4. In the **Rule Editor**, click **Action** > **Import**.

   The **Import** window opens.

5. Navigate to the following directory:

   `<Dynamic Data Masking installation>\Accelerators\ActiveDirectory\rules`

6. Select the LDAPRuleSet.xml file and click **Import**.

   The MatchTables rule folder appears in the **Rule Editor**.

7. Expand the MatchTables rule folder to view the LDAPActualUser rule and the BlackList and WhiteList rule folders.

8. Expand the BlackList folder to view the BlackList rules.

9. Select the MaskIfLDAPMatch rule and click **Action** > **Edit**.

   The **Edit Rule** window opens.

10. In the class path field of the rule matcher, enter the file path to LDAP.jar.

    You can find LDAP.jar in the following location:
    `<Dynamic Data Masking installation>\Accelerators\ActiveDirectory\lib\LDAP.jar`

    Note: You must enter the correct class path even if you disable the MaskIfLDAPMatch rule. The Rule Engine reads every rule in the rule set and returns an error if the class path is incorrect.

11. Click **OK**.

    The **Rule Editor** closes.

12. Expand the WhiteList folder to view the WhiteList rules.

13. Select the StopIfLDAPMatch rule and click **Action** > **Edit**.

    The **Edit Rule** window opens.

14. In the class path field of the rule matcher, enter the file path to the LDAP.jar file.

    You can find the LDAP.jar file in the following location:
    `<Dynamic Data Masking installation>\Accelerators\ActiveDirectory\lib\LDAP.jar`

    Note: You must enter the correct class path even if you disable the StopIfLDAPMatch rule. The Rule Engine reads every rule in the rule set and returns an error if the class path is incorrect.

15. Click **OK**.

    The **Rule Editor** closes.

16. Define tables with sensitive information in the MatchTables rule folder.

17. Define LDAP users in the LDAPActualUser rule or disable the rule to mask data based on user groups or attributes you define in the BlackList and WhiteList rules.

18. Define BlackList and WhiteList groups or attributes in the **Rule Editor**. Select a rule and click **Action** > **Edit** to open the **Edit Rule** window.

19. Click **File** > **Update Rules** to save the security rules.

20. Click **File** > **Exit** to close the **Rule Editor**.

CHAPTER 3

Active Directory Accelerator Rules

This chapter includes the following topics:

Active Directory Accelerator Rules Overview

The Active Directory accelerator contains the LDAP Rule Set security rule set. The rule set contains rules and rule folders that you configure to mask data based on the LDAP user, attribute, or group.

If you want to define an LDAP user that receives masked or unmasked data, define the user in the LDAPActualUser rule.

If you want to define LDAP groups that receive masked data or users with LDAP attribute values that you want to receive masked data, enable the BlackList folder and disable the WhiteList folder. Use the BlackListGroups rule to mask data based on LDAP groups. Use the BlackListAttributeName and BlackListAttributeValues rules to mask data based on attribute values.

If you want some LDAP groups to receive unmasked data or you want users with certain LDAP attribute values to receive unmasked data, enable the WhiteList folder and disable the BlackList folder. Use the WhiteListGroups rule to allow users in an LDAP group to view unmasked data. The groups that you define in the WhiteListGroups rule receive unmasked data. The groups that you do not list in the WhiteListGroups rule view masked data. Use the WhiteListAttributeName and WhiteListAttributeValues rules to allow users with certain LDAP attribute values to view unmasked data.

Note: Disable the BlackList or WhiteList rule folder based on how you want to mask data. If you enable the BlackList rule folder and the WhiteList rule folder, the SQL request goes to the first folder in the tree.

Connection Rule

A Dynamic Data Masking connection rule directs the SQL request to the LDAP Rule Set security rule set.

You must create a connection rule in the Dynamic Data Masking Management Console to use the Active Directory accelerator. Configure the connection rule to identify the incoming connection by the database name. Select the Use Rule Set action and define the LDAP Rule Set rule set name. Select the Stop if Applied processing action. If a request is made to the database, the Rule Engine will apply the LDAP Rule Set.

MatchTables Rule

The MatchTables rule is a security rule folder that defines the names of the tables that contain sensitive information.

To use the LDAP Rule Set, you must enable the MatchTables rule. Select the Text security rule matcher and define the tables that you want to mask in the Text field. The MatchTables rule uses the Folder rule action to direct the Rule Engine to the rules in the MatchTables rule folder.

The following table describes the rules in the MatchTables folder:

Rule	Description
LDAPActualUser	Defines the LDAP user that receives masked or unmasked data.
BlackList	Rule folder that contains the rules that define the LDAP groups that receive masked data or the attributes of users that receive masked data.
WhiteList	Rule folder that contains the rules that define the LDAP groups that receive unmasked data or the attributes of users that receive unmasked data.

LDAPActualUser Rule

LDAPActualUser is a security rule that defines a user that receives masked or unmasked data and defines the LDAP_ACTUAL_USER symbol.

You do not need to define the LDAP_ACTUAL_USER symbol if the value of the AUTH_SID global symbol is set to the correct user. The LDAP matcher uses the AUTH_SID symbol if you do not define the LDAP_ACTUAL_USER symbol. If the AUTH_SID symbol is not defined, you must define the LDAP_ACTUAL_USER symbol in the LDAPAcutalUser rule.

The LDAPActualUser rule uses the Continue processing action. Enable the BlackList or WhiteList rule folder to determine whether the user you define in the LDAPActualUser rule receives masked or unmasked data.

BlackList Rules

The BlackList rule is a rule folder that defines LDAP groups or users with LDAP attribute values that receive masked data.

To use the BlackList masking method, enable the BlackList rule folder and disable the WhiteList rule folder.

The BlackList rule folder contains BlackListGroups, BlackListAttributeName, BlackListAttributeValue, and MaskIfLDAPMatch rules.

If you want to mask data based on the LDAP group of a user, enable the BlackListGroups rule and disable the BlackListAttributeName and BlackListAttributeValues rules. You define the LDAP groups that receive masked data in the BlackListGroups rule and set the Groups symbol value to the list of the LDAP groups. Enter the LDAP groups that receive masked data in the Symbol Value field. Separate groups with a pipe symbol (|).

If you want to mask data based on the LDAP attribute values of users, disable the BlackListGroups rule and enable the BlackListAttributeName and BlackListAttributeValues rules. Define the attribute in the BlackListAttributeName rule. Set the ATTR_NAME Symbol Value to the name of the attribute. In the BlackListAttributeValues rule, define the attribute values of the attribute that you specified in the BlackListAttributeName rule. Set the ATTR_VALUES Symbol Value to the attribute values that you use to identify a user that receives masked data.

You must identify users that receive masked data based on the LDAP group or attribute values. You cannot identify LDAP groups and attribute values. If you enable the BlackListGroups rule, the LDAP matcher does not verify the values of the ATTR_NAME and ATTR_VALUES that you define in the BlackListAttribueName and BlackListAttributeValues rules.

Configure the MaskIfLDAPMatch rule to define how to mask the data. The rule contains table columns that commonly contain personally identifiable information. Modify the rule based on the data that you want to mask.

The following table describes the BlackList rules:

Rule	Description
BlackListGroups	Defines the value of the Groups symbol. Enter the LDAP groups that you want to receive masked data. You cannot use the BlackListGroups rule with the BlackListAttributeName and BlackListAttribueValues rules.
BlackListAttributeName	Defines the ATTR_NAME symbol. Enter the LDAP attribute that you use to identify users that receive masked data. You cannot use the BlackListAttributeName rule with the BlackListGroups rule.
BlackListAttributeValues	Defines the ATTR_VALUES symbol. Enter the LDAP attribute values that you use to identify users that receive masked data. You cannot use the BlackListAttributeName rule with the BlackListGroups rule.
MaskIfLDAPMatch	Defines how to mask the sensitive data.

WhiteList Rules

The WhiteList rule is a rule folder that defines the LDAP groups or attribute values of users that receive unmasked data. Dynamic Data Masking masks data for LDAP groups and users that do not return a match in the WhiteList rules.

To use the WhiteList masking method, enable the WhiteList rule folder and disable the BlackList rule folder.

The WhiteList rule folder contains WhiteListGroups, WhiteListAttributeName, WhiteListAttributeValues, StopIfLDAPMatch, and MaskingRule rules.

If you want to define LDAP groups that do not receive masked data, enable the WhiteListGroups rule and disable the WhiteListAttributeName and WhiteListAttributeValues rules. In the WhiteListGroups rule, set the Groups symbol value to the list of LDAP groups that receive unmasked data. Enter the LDAP groups that receive unmasked data in the Symbol Value field. Separate groups with a pipe symbol (|).

If you want to define users that receive unmasked data based on the LDAP attribute values of the users, disable the WhiteListGroups rule and enable the WhiteListAttributeName and WhiteListAttributeValues rules. Define the attribute in the WhiteListAttributeName rule. Set the ATTR_NAME Symbol Value to the name of the attribute. In the WhiteListAttributeValues rule, define the attribute values of the attribute that you specified in the WhiteListAttributeName rule. Set the ATTR_VALUES Symbol Value to the attribute values that you use to identify a user that receives unmasked data.

The StopIfLDAPMatch rule uses a Stop rule action if the LDAP group or attribute value is a match. The Rule Engine does not apply the MaskingRule rule and the user receives unmasked data.

Configure the MaskingRule rule to define how to mask the data. The rule contains columns that commonly contain personally identifiable information. Modify the rule based on the data that you want to mask.

The following table describes the WhiteList rules:

Rule	Description
WhiteListGroups	Defines the value of the Groups symbol. Enter the LDAP groups that you want to receive unmasked data. You cannot use the WhiteListGroups rule with the WhiteListAttributeName and WhiteListAttribueValues rules.
WhiteListAttributeName	Defines the ATTR_NAME symbol. Enter the LDAP attribute that you use to identify users that receive unmasked data. You cannot use the WhiteListAttributeName rule with the WhiteListGroups rule.
WhiteListAttributeValues	Defines the ATTR_VALUES symbol. Enter the LDAP attribute values that you use to identify users that receive unmasked data. You cannot use the WhiteListAttributeName rule with the WhiteListGroups rule.
StopIfLDAPMatch	Stops the Rule Engine. The Rule Engine does not apply the MaskingRule rule if the StopIfLDAPMatch rule returns a match.
MaskingRule	Defines how to mask the sensitive data.

CHAPTER 4

Debug the Active Directory Accelerator

This chapter includes the following topics:

Debug the Active Directory Accelerator Overview

You can debug the LDAP matcher before you use it with Dynamic Data Masking.

The LDAP debug mode does not use a security rule set. The debug mode allows you do define the LDAP_ACTUAL_USER, ATTR_NAME, ATTR_VALUES, and Groups symbols to determine whether the LDAP matcher correctly matches the Groups symbol or the ATTR_NAME and ATTR_VALUES symbols for the LDAP_ACTUAL_USER user.

When you run the accelerator standalone, you create output files that show the message outputs for LDAP group matching and attribute values matching. When you run the accelerator with the Dynamic Data Masking Server, you enable the debug log level that logs detailed information to the server.log file.

Compare the output files to verify that the Active Directory Accelerator runs with and without the Dynamic Data Masking Server.

The following text shows an example of the debug information from the server.log file:

```
12/05 16:03:50,829 [DDM for Oracle-2] DEBUG - Match User according to Attribute
countryCode and Attribute Values 123|456|789
12/05 16:03:50,838 [DDM for Oracle-2] DEBUG - Attribute userPrincipalName:
user@company.com
12/05 16:03:50,838 [DDM for Oracle-2] DEBUG - Attribute userPrincipalName has 1 values
12/05 16:03:50,838 [DDM for Oracle-2] DEBUG - Attribute description: Team Lead
12/05 16:03:50,838 [DDM for Oracle-2] DEBUG - Attribute description has 1 values
12/05 16:03:50,838 [DDM for Oracle-2] DEBUG - Attribute showInAddressBook: CN=Default
Global Address List,CN=All Global Address Lists,CN=Address Lists
Container,CN=Company,CN=Microsoft
Exchange,CN=Services,CN=Configuration,DC=Company,DC=com, CN=All Users,CN=All Address
Lists,CN=Address Lists Container,CN=Company,CN=Microsoft
Exchange,CN=Services,CN=Configuration,DC=Company,DC=com
12/05 16:03:50,838 [DDM for Oracle-2] DEBUG - Attribute showInAddressBook has 2 values
12/05 16:03:50,838 [DDM for Oracle-2] DEBUG - Attribute mailNickname: user
12/05 16:03:50,838 [DDM for Oracle-2] DEBUG - Attribute mailNickname has 1 values
12/05 16:03:50,838 [DDM for Oracle-2] DEBUG - Attribute homeDirectory: \\\home\user
12/05 16:03:50,838 [DDM for Oracle-2] DEBUG - Attribute homeDirectory has 1 values
```

```
12/05 16:03:50,838 [DDM for Oracle-2] DEBUG - Attribute homeDrive: U:
12/05 16:03:50,838 [DDM for Oracle-2] DEBUG - Attribute homeDrive has 1 values
12/05 16:03:50,838 [DDM for Oracle-2] DEBUG - Attribute uSNChanged: 12345678
12/05 16:03:50,838 [DDM for Oracle-2] DEBUG - Attribute uSNChanged has 1 values
.....
12/05 16:03:50,842 [DDM for Oracle-2] DEBUG - Attribute userAccountControl has 1 values
12/05 16:03:50,843 [DDM for Oracle-2] DEBUG - Attribute location: City
12/05 16:03:50,843 [DDM for Oracle-2] DEBUG - Attribute location has 1 values
12/05 16:03:50,843 [DDM for Oracle-2] DEBUG - **************************
12/05 16:03:50,843 [DDM for Oracle-2] DEBUG - Value 123 of attribute countryCode found
12/05 16:03:50,843 [DDM for Oracle-2] DEBUG - LDAP returns TRUE
```

Debugging the Active Directory Accelerator

Debug the Active Directory accelerator.

1. Navigate to the following directory:

   ```
   <Dynamic Data Masking installation>/Accelerators/ActiveDirectory/cfg
   ```

2. Find the sample_ldap.properties file and save the file as ldap.properties in the following directory:

   ```
   <Dynamic Data Masking installation>/custom/cfg
   ```

3. Edit the following properties in the ldap.properties file:

   hostname

   The host name or IP address of the LDAP directory.

   port

   The LDAP port. Default is 389.

   authentication

   The LDAP authentication. The authentication can be simple or none.

   basedn

   The domain name in the LDAP directory format. For example, if the domain name is mycompany.com, enter the following text:

   ```
   basedn=DC\=mycompany,DC\=com
   ```

   principal

   The user name that connects to the LDAP directory followed by @<domain name>, such as jsmith@mycompany.com. Required if you configure the authentication to be simple.

   rootpwd

   The password of the user that connects to the LDAP directory. Required if you configure the authentication to be simple.

   PRINT_TO_OUTPUT

   Enter enabled.

   LDAP_ACTUAL_USER

   Enter the LDAP user that you want to check.

   ATTR_NAME

   Enter the attribute name that you want to check.

ATTR_VALUES

Enter the attribute values that you want to check, separated by a vertical bar (|).

Groups

Enter the groups that you want to check, separated by a vertical bar (|).

4. Save the file in the custom/cfg directory as ldap.properties.
5. Find the ldap.bat file for Windows or the ldap file for Linux and UNIX. You can find the file in the following location:

   ```
   <Dynamic Data Masking installation>/Accelerators/ActiveDirectory/lib
   ```
6. Copy the ldap.bat file or the ldap file to the Dynamic Data Masking installation directory.
7. In a command prompt, navigate to the Dynamic Data Masking installation directory.
8. Run the following command in the command prompt:
   - On Windows run the following command:

     ```
     ldap.bat > myOutput.out
     ```
   - On Linux and UNIX, run the following command:

     ```
     ldap > myOutput.out
     ```

   A myOutput.out file appears in the installation directory with output messages for the LDAP matcher.
9. Save the myOutput.out file.
10. Open the ldap.properties file and comment-out the Groups property. Enter a pound sign (#) before the Groups property.
11. Save the ldap.properties file and run the following command in the command prompt:
    - On Windows run the following command:

      ```
      ldap.bat > myOutput.out
      ```
    - On Linux and UNIX, run the following command:

      ```
      ldap > myOutput.out
      ```

    A myOutput.out file appears in the lib directory with output messages for the attribute value matcher.

Debugging the Active Directory Accelerator with the Dynamic Data Masking Server

Debug the Active Directory accelerator with the Dynamic Data Masking Server

1. Navigate to the following directory:

   ```
   <Dynamic Data Masking installation>/Accelerators/ActiveDirectory/cfg
   ```
2. Find the sample_ldap.properties file and save the file as ldap.properties in the following directory:

   ```
   <Dynamic Data Masking installation>/custom/cfg
   ```
3. Edit the following properties in the ldap.properties file:

   hostname

   The host name or IP address of the LDAP directory.

port

The LDAP port. Default is 389.

authentication

The LDAP authentication. The authentication can be simple or none.

basedn

The domain name in the LDAP directory format. For example, if the domain name is mycompany.com, enter the following text:

```
basedn=DC\=mycompany,DC\=com
```

principal

The user name that connects to the LDAP directory followed by @<domain name>, such as jsmith@mycompany.com. Required if you configure the authentication to be simple.

rootpwd

The password of the user that connects to the LDAP directory. Required if you configure the authentication to be simple.

4. In the ldap.properties file, comment-out the following properties with a pound sign (#) at the beginning of each line:
   - PRINT_TO_OUTPUT
   - LDAP_ACTUAL_USER
   - ATTR_NAME
   - ATTR_VALUES
   - Groups
5. Save the file in the custom/cfg directory as ldap.properties.
6. Navigate to the following directory:

   ```
   <Dynamic Data Masking installation>/cfg
   ```
7. Find the config.properties file. Back up the file before you make any changes.
8. Set the log level to debug. Edit the following property:

   ```
   TraceFacility.logLevel=debug
   ```
9. Restart the Dynamic Data Masking Server.
10. Open the LDAPRuleSet in the Management Console. Verify that you defined the LDAP.jar location, LDAP_ACTUAL_USER, ATTR_NAME, and ATTR_VALUES symbols correctly.
11. In a Dynamic Data Masking client, verify that the masking rules work.
12. Navigate to the following directory:

    ```
    <Dynamic Data Masking installation>/log
    ```
13. Open the server.log file and verify that it contains the same information as the myOutput.out file you created when you tested the Active Directory accelerator without the Dynamic Data Masking Server.

INDEX