IBM Security Verify Identity
7.0

LDAP Adapter Installation and Configuration Guide

Contents

Figures

Tables

Chapter 1. Overview

An adapter is an interface between a managed resource and the Identity server. The LDAP Adapter enables communication between the Identity server and a network of systems that run IBM Directory Server or Sun ONE Directory Server.

Adapters can be installed on the managed resource. The Identity server manages access to the resource by using the security system. Adapters function as trusted virtual administrators on the target operating system. The adapter creates, suspends, restores user accounts, and other functions that administrators run manually. The adapter runs as a service, independently of whether you are logged on to the Identity server.

Features of the adapter

The adapter automates several administrative and management tasks.

- Reconciling user accounts and other support data
- Adding user accounts
- Modifying user account attributes
- Modifying user account passwords
- Suspending, restoring, and deleting user accounts
- Adding, modifying, and deleting groups

Related concepts

Architecture of the adapter
Several components are involved in running and using the adapter. Install all these components so that the adapter can function correctly.

Supported configurations
The adapter supports both single and multiple server configurations.

Architecture of the adapter

Several components are involved in running and using the adapter. Install all these components so that the adapter can function correctly.

- RMI Dispatcher
- Security Directory Integrator connector
- IBM® Security Verify Adapter profile

You need to install the Remote Method Invocation (RMI) Dispatcher and the adapter profile; however, the Security Directory Integrator connector might already be installed with the base Security Directory Integrator product.

Figure 1 on page 2 describes the components that work together to complete the user account and group management tasks in a Security Directory Integrator environment.

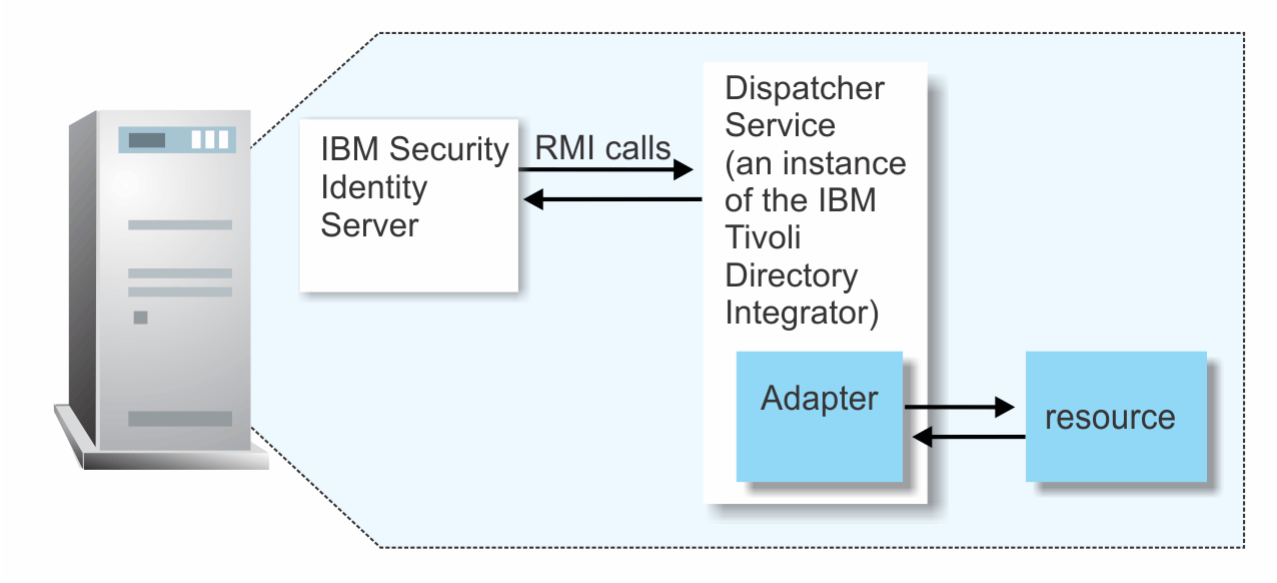

Figure 1. The architecture

Related concepts

Features of the adapter
The adapter automates several administrative and management tasks.

Supported configurations
The adapter supports both single and multiple server configurations.

Supported configurations

The adapter supports both single and multiple server configurations.

- The Identity server
- The Tivoli® Directory Integrator server
- The managed resource
- The adapter

The adapter must reside directly on the server running the Security Directory Integrator server.

Single server configuration

In a single server configuration, install the Identity server, the Security Directory Integrator server, and the LDAP Adapter on one server to establish communication with the IBM Directory Server or Sun ONE Directory Server.

The IBM Directory Server or Sun ONE Directory Server is installed on a different server as described in Figure 2 on page 3.

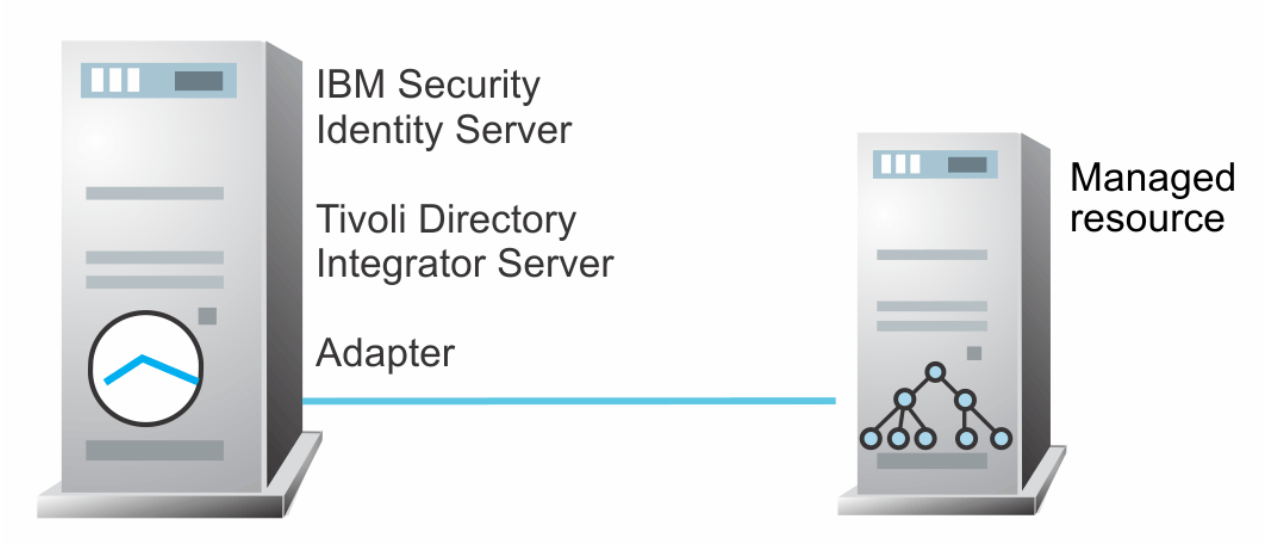

Figure 2. Example of a single server configuration

Multiple server configuration

In a multiple server configuration, the Identity server, the Security Directory Integrator server, the LDAP Adapter, and the IBM Directory Server or Sun ONE Directory Server are installed on different servers.

Install the Security Directory Integrator server and the LDAP Adapter on the same server as described in Figure 3 on page 3.

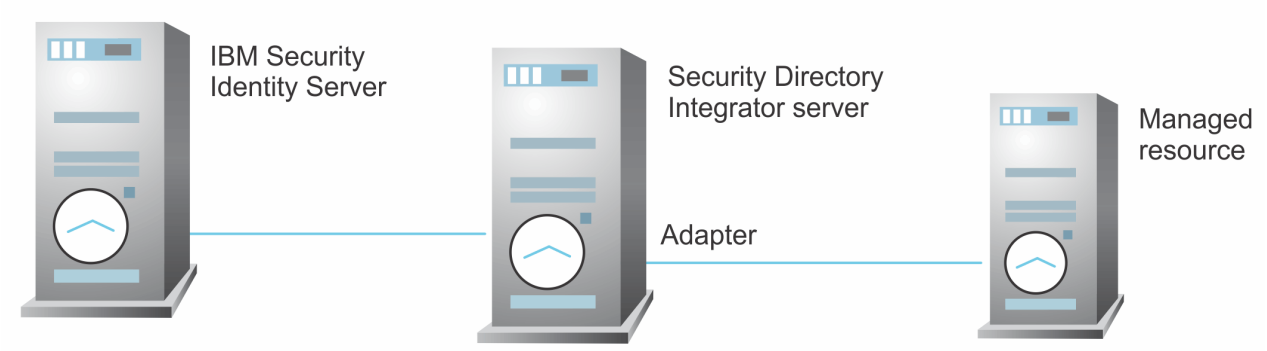

Figure 3. Example of multiple server configuration

Related concepts

Features of the adapter
The adapter automates several administrative and management tasks.

Architecture of the adapter
Several components are involved in running and using the adapter. Install all these components so that the adapter can function correctly.

Chapter 2. Planning

Installing and configuring the adapter involves several steps that you must complete in a specific sequence. Follow the roadmap for the main tasks.

Roadmap for IBM Security Directory Integrator based adapters, for IBM Security Verify Identity 7.x

Follow this section when using the guide to install, configure, troubleshoot, or uninstall the adapter.

Pre-installation

Complete these tasks.

1. Verify that your environment meets the software and hardware requirements for the adapter. See *Prerequisites*.
2. Obtain the installation software. See *Software downloads*.
3. Obtain the necessary information for the installation and configuration. See *Installation worksheet*.

Installation

Complete these tasks.

1. Install the dispatcher.
2. Install the adapter binaries or connector.
3. Install 3rd party client libraries.
4. Set up the adapter environment.
5. Restart the adapter service.
6. Import the adapter profile.
7. Create an adapter service/target.
8. Install the adapter language package.
9. Verify that the adapter is working correctly.

Upgrade

To upgrade the adapter, do a full installation of the adapter. Follow the *Installation roadmap*.

Configuration

Complete these tasks.

1. Configure secure communication between the Identity server and the adapter.
    a. Configure 1-way authentication.
    b. Configure 2-way authentication.
2. Configure secure communication between the adapter and the managed target.
    a. Configure 1-way authentication.
    b. Configure 2-way authentication.
3. Configure the adapter.
4. Modify the adapter profiles.
5. Customize the adapter.

Troubleshooting

See the following topics.

- Techniques for troubleshooting problems
- Configure debugging
- Logs
- Error messages and problem solving

Uninstallation

Complete these tasks.

1. Stop the adapter service.
2. Remove the adapter binaries or connector.
3. Remove 3rd party client libraries.
4. Delete the adapter service/target.
5. Delete the adapter profile.

Reference

See the following topics.

- Adapter attributes and object classes
- Adapter attributes by operations
- Special attributes

Related concepts

Prerequisites
Verify that your environment meets the software and hardware requirements for the adapter.

Software downloads
Download the software through your account at the IBM Passport Advantage website.

Installation worksheet
The installation worksheet lists the information that is required to install and configure the adapter. Complete this worksheet before you start the installation procedure for ease of reference. Make a copy of the worksheet for each adapter instance you install.

Prerequisites

Verify that your environment meets the software and hardware requirements for the adapter.

Table 1 on page 7 identifies the software and operating system prerequisites for the adapter installation.

Ensure that you install the adapter on the same workstation as the Security Directory Integrator server.

Table 1. Requirements to run the adapter	
Prerequisite	**Description**
Directory Integrator	• IBM Security Directory Integrator Version 7.1.1 + 7.1.1-TIV-TDI-FP0004 + 7.2.0-ISS-SDI-LA0008 • IBM Security Directory Integrator Version 7.2 **Note:** • Earlier versions of IBM Security Directory Integrator that are still supported might function properly. However, to resolve any communication errors, you must upgrade your Directory Integrator release to the versions that the adapter officially supports. • The adapter supports IBM Security Directory Integrator 7.2, which is available only to customers who have the correct entitlement. Contact your IBM representative to find out whether you have the entitlement to download IBM Security Directory Integrator 7.2.
Identity server	The following servers are supported: • Identity server Version 10.0 • Identity server Version 10.0 • IBM Security Privileged Identity Manager Version 2.0 • Identity server Version 10.0
Directory server	• IBM Security Directory Server version 6.2 • Sun Directory Server version 6.3 • Directory servers that comply with RFC2798 standards and supported by the Security Directory Integrator LDAP connector. You might require additional customization.
System Administrator Authority	To complete the adapter installation procedure, you must have system administrator authority.
Security Directory Integrator adapters solution directory	A Security Directory Integrator adapters solution directory is a Security Directory Integrator work directory for adapters. See the *Dispatcher Installation and Configuration Guide*.

For information about the prerequisites and supported operating systems for Security Directory Integrator, see the *IBM Tivoli Directory Integrator 7.1: Administrator Guide*.

Related concepts

Roadmap for IBM Security Directory Integrator based adapters, for IBM Security Verify Identity 7.x
Follow this section when using the guide to install, configure, troubleshoot, or uninstall the adapter.

Software downloads
Download the software through your account at the IBM Passport Advantage website.

Installation worksheet

The installation worksheet lists the information that is required to install and configure the adapter. Complete this worksheet before you start the installation procedure for ease of reference. Make a copy of the worksheet for each adapter instance you install.

Software downloads

Download the software through your account at the IBM Passport Advantage website.

Go to IBM Passport Advantage.

See the corresponding *IBM Security Verify Identity Download Document* for instructions.

Note:

You can also obtain additional adapter information from IBM Support.

Related concepts

Roadmap for IBM Security Directory Integrator based adapters, for IBM Security Verify Identity 7.x
Follow this section when using the guide to install, configure, troubleshoot, or uninstall the adapter.

Prerequisites
Verify that your environment meets the software and hardware requirements for the adapter.

Installation worksheet
The installation worksheet lists the information that is required to install and configure the adapter. Complete this worksheet before you start the installation procedure for ease of reference. Make a copy of the worksheet for each adapter instance you install.

Installation worksheet

The installation worksheet lists the information that is required to install and configure the adapter. Complete this worksheet before you start the installation procedure for ease of reference. Make a copy of the worksheet for each adapter instance you install.

Table 2 on page 8 identifies the information that you need before installing the adapter.

Table 2. Required information to install the adapter

Required information	Description	Value

Security Directory Integrator Home Directory	The *ITDI_HOME* directory contains the jars/connectors subdirectory that contains files for the adapters. For example, the jars/connectors subdirectory contains the files for the UNIX adapter.	If Security Directory Integrator is automatically installed with your IBM Security Verify Identity product, the default directory path for Security Directory Integrator is as follows:
		Windows
		• for version 7.1:
		`drive\Program Files \IBM\TDI\V7.1`
		UNIX
		• for version 7.1:
		`/opt/IBM/TDI/V7.1`

Table 2. Required information to install the adapter (continued)		
Required information	**Description**	**Value**

Solution Directory	This directory is the default directory. When you install the dispatcher, the adapter prompts you to specify a file path for the solution directory. For more information about the solution directory, see the *Dispatcher Installation and Configuration Guide*.	**Windows**
		• for version 7.1:
		`drive\Program Files \IBM\TDI\V7.1\timsol`
		UNIX
		• for version 7.1:
		`/opt/IBM/TDI/V7.1/ timsol`

Related concepts

Roadmap for IBM Security Directory Integrator based adapters, for IBM Security Verify Identity 7.x
Follow this section when using the guide to install, configure, troubleshoot, or uninstall the adapter.

Prerequisites
Verify that your environment meets the software and hardware requirements for the adapter.

Software downloads
Download the software through your account at the IBM Passport Advantage website.

Chapter 3. Installing

Installing the adapter mainly involves importing the adapter profile and creating an adapter service. Depending on the adapter, several other tasks can be involved to completely install it.

All IBM Security Directory Integrator based adapters require the Dispatcher for the adapters to function correctly. If the Dispatcher is installed from a previous installation, do not reinstall it unless the Dispatcher is upgraded. See Installing the dispatcher.

Depending on your adapter, the Security Directory Integrator connector might already be installed as part of the Security Directory Integrator product and no further action is required. If the connector is not pre-installed, install it after the Dispatcher.

Installing the dispatcher

If this is the first Security Directory Integrator-based adapter installation, you must install the RMI Dispatcher before you install the adapter. Install the RMI Dispatcher on the same Security Directory Integrator server where you want to install the adapter.

If you already installed the RMI Dispatcher for another adapter, you do not need to reinstall it.

If you have not yet installed the RMI Dispatcher in the Security Directory Integrator environment, download the Dispatcher installer from the IBM Passport Advantage website. For more information about the installation, see the *Dispatcher Installation and Configuration Guide*.

Related concepts

Restarting the adapter service
Various installation and configuration tasks might require the adapter to be restarted to apply the changes. For example, you must restart the adapter if there are changes in the adapter profile, connector, or assembly lines. To restart the adapter, restart the Dispatcher.

Service/Target form details
Complete the service/target form fields.

Installing the adapter language package
The adapters use a separate language package from IBM Security Verify Identity.

Related tasks

Installing the adapter binaries or connector
The connector might or might not be available with the base Security Directory Integrator or Security Directory Integrator product. The connector is required to establish communication between the adapter and the Dispatcher.

Importing the adapter profile
An adapter profile defines the types of resources that the Identity server can manage. It is packaged with the IBM Security Verify Adapter. Use the adapter profile to create an adapter service on Identity server and establish communication with the adapter.

Creating an adapter service/target
After you import the adapter profile on the Identity server, create a service/target so that Identity server can communicate with the managed resource.

Verifying that the adapter is working correctly

After you install and configure the adapter, verify that the installation and configuration are correct.

Installing the adapter binaries or connector

The connector might or might not be available with the base Security Directory Integrator or Security Directory Integrator product. The connector is required to establish communication between the adapter and the Dispatcher.

Before you begin

- The Dispatcher must be installed.

About this task

The adapter uses the IBM Security Directory Integrator JDBC connector. Follow the steps in the procedure to to download and copy the JDBC Connector JAR. As such, you just need to install the Dispatcher. See the *IBM Security Dispatcher Installation and Configuration Guide*..

Related concepts

Installing the dispatcher
If this is the first Security Directory Integrator-based adapter installation, you must install the RMI Dispatcher before you install the adapter. Install the RMI Dispatcher on the same Security Directory Integrator server where you want to install the adapter.

Restarting the adapter service
Various installation and configuration tasks might require the adapter to be restarted to apply the changes. For example, you must restart the adapter if there are changes in the adapter profile, connector, or assembly lines. To restart the adapter, restart the Dispatcher.

Service/Target form details
Complete the service/target form fields.

Installing the adapter language package
The adapters use a separate language package from IBM Security Verify Identity.

Related tasks

Importing the adapter profile
An adapter profile defines the types of resources that the Identity server can manage. It is packaged with the IBM Security Verify Adapter. Use the adapter profile to create an adapter service on Identity server and establish communication with the adapter.

Creating an adapter service/target
After you import the adapter profile on the Identity server, create a service/target so that Identity server can communicate with the managed resource.

Verifying that the adapter is working correctly
After you install and configure the adapter, verify that the installation and configuration are correct.

Restarting the adapter service

Various installation and configuration tasks might require the adapter to be restarted to apply the changes. For example, you must restart the adapter if there are changes in the adapter profile, connector, or assembly lines. To restart the adapter, restart the Dispatcher.

The adapter does not exist as an independent service or a process. The adapter is added to the Dispatcher instance, which runs all the adapters that are installed on the same Security Directory Integrator instance.

See the topic about starting, stopping, and restarting the Dispatcher service in the *Dispatcher Installation and Configuration Guide*.

Related concepts

Installing the dispatcher
If this is the first Security Directory Integrator-based adapter installation, you must install the RMI Dispatcher before you install the adapter. Install the RMI Dispatcher on the same Security Directory Integrator server where you want to install the adapter.

Service/Target form details
Complete the service/target form fields.

Installing the adapter language package
The adapters use a separate language package from IBM Security Verify Identity.

Related tasks

Installing the adapter binaries or connector
The connector might or might not be available with the base Security Directory Integrator or Security Directory Integrator product. The connector is required to establish communication between the adapter and the Dispatcher.

Importing the adapter profile
An adapter profile defines the types of resources that the Identity server can manage. It is packaged with the IBM Security Verify Adapter. Use the adapter profile to create an adapter service on Identity server and establish communication with the adapter.

Creating an adapter service/target
After you import the adapter profile on the Identity server, create a service/target so that Identity server can communicate with the managed resource.

Verifying that the adapter is working correctly
After you install and configure the adapter, verify that the installation and configuration are correct.

Importing the adapter profile

An adapter profile defines the types of resources that the Identity server can manage. It is packaged with the IBM Security Verify Adapter. Use the adapter profile to create an adapter service on Identity server and establish communication with the adapter.

Before you begin

- You have root or administrator authority on the Identity server.
- The file to be imported must be a Java™ archive (JAR) file. The `<Adapter>Profile.jar` file includes all the files that are required to define the adapter schema, account form, service/target form, and profile properties. If necessary, you can extract the files from the JAR file, modify the files, and repackage the JAR file with the updated files.The JAR file for IBM Security Identity Manager is located in the top level folder of the installation package.

About this task

Service definition files are also called adapter profile files.

If the adapter profile is not installed correctly, the adapter cannot function correctly. You cannot create a service with the adapter profile or open an account on the service. You must import the adapter profile again.

Procedure

1. Log on to the Identity server by using an account that has the authority to perform administrative tasks.
2. From the navigation tree, select **Configure System** > **Manage Service Types**.
   The **Manage Service Types** page is displayed.
3. On the **Manage Service Types** page, click **Import**.

The **Import Service Type** page is displayed.

4. On the **Import Service Type** page, complete these steps:
   a) In the **Service Definition File** field, type the directory location of the *<Adapter>*`Profile.jar` file, or click **Browse** to locate the file.
   For example, if you are installing the IBM Security Verify Adapter for a Windows server that runs Active Directory, locate and import the `ADProfileJAR` file.
   b) Click **OK** to import the file.

Results

A message indicates that you successfully submitted a request to import a service type.

What to do next

- The import occurs asynchronously, which means it might take some time for the service type to load into the Identity server from the properties files and to be available in other pages. On the **Manage Service Types** page, click **Refresh** to see the new service type. If the service type status is `Failed`, check the log files to determine why the import failed.
- If you receive a schema-related error, see the `trace.log` file for information about it. The `trace.log` file location is specified by the **`handler.file.fileDir`** property that is defined in the `enRoleLogging.properties` file. The `enRoleLogging.properties` file is in the Identity server*HOME*`\data` directory. .

Related concepts

Installing the dispatcher
If this is the first Security Directory Integrator-based adapter installation, you must install the RMI Dispatcher before you install the adapter. Install the RMI Dispatcher on the same Security Directory Integrator server where you want to install the adapter.

Restarting the adapter service
Various installation and configuration tasks might require the adapter to be restarted to apply the changes. For example, you must restart the adapter if there are changes in the adapter profile, connector, or assembly lines. To restart the adapter, restart the Dispatcher.

Service/Target form details
Complete the service/target form fields.

Installing the adapter language package
The adapters use a separate language package from IBM Security Verify Identity.

Related tasks

Installing the adapter binaries or connector
The connector might or might not be available with the base Security Directory Integrator or Security Directory Integrator product. The connector is required to establish communication between the adapter and the Dispatcher.

Creating an adapter service/target
After you import the adapter profile on the Identity server, create a service/target so that Identity server can communicate with the managed resource.

Verifying that the adapter is working correctly

After you install and configure the adapter, verify that the installation and configuration are correct.

Creating an adapter service/target

After you import the adapter profile on the Identity server, create a service/target so that Identity server can communicate with the managed resource.

Before you begin

Complete "Importing the adapter profile" on page 13.

About this task

You must create an administrative user account for the adapter on the managed resource. You can provide the account information such as administrator name and password when you create the adapter service. Ensure that the account has sufficient privileges to administer the users. For information about creating an administrative account, see the documentation for the managed resource.

To create or change a service, you must use the service form to provide information for the service. Service forms might vary depending on the adapter. The service name and description that you provide for each service are displayed on the console. Therefore, it is important to provide values that make sense to your users and administrators.

Procedure

1. From the navigation tree, click **Manage Services**.
   The **Select a Service** page is displayed.
2. On the **Select a Service** page, click **Create**.
   The **Create a Service** wizard is displayed.
3. On the **Select the Type of Service** page, click **Search** to locate a business unit.
   The **Business Unit** page is displayed.
4. On the **Business Unit** page, complete these steps:
   a) Type information about the business unit in the **Search information** field.
   b) Select a business type from the **Search by** list, and then click **Search**.
      A list of business units that matches the search criteria is displayed.
      If the table contains multiple pages, you can do the following tasks:
      - Click the arrow to go to the next page.
      - Type the number of the page that you want to view and click **Go**.
   c) In the **Business Units** table, select business unit in which you want to create the service, and then click **OK**.
      The **Select the Type of Service** page is displayed, and the business unit that you specified is displayed in the **Business unit** field.
5. On the **Select the Type of Service** page, select a service type, and then click **Next**.
   If the table contains multiple pages, you can do the following tasks:
   - Click the arrow to go to the next page.
   - Type the number of the page that you want to view and click **Go**.
6. On either the **Service Information** or **General Information** page, specify the appropriate values for the service instance.
   The content of the **General Information** page depends on the type of service that you are creating. The creation of some services might require more steps.
7. To create a service with NTLM authentication, the administrator login is in the following format:

```
<Domain Name>\<Login Name>
```

8. For NLTM authentication, select **Authentication** mode as 'Claims-Based Authentication.
9. On the **Dispatcher Attributes** page, specify information about the dispatcher attributes, and then click **Next** or **OK**.

   The **Dispatcher Attributes** page is displayed only for IBM Security Directory Integrator based services.
10. Optional: On the **Access Information** page, select the **Define an Access** check box to activate the access definition fields. Select the type of access you want to enable.

    Specify the expected access information and any other optional information such as description, search terms, more information, or badges.
11. On the **Status and Information** page, view information about the adapter and managed resource, and then click **Next** or **Finish**.

    The adapter must be running to obtain the information.
12. On the **Configure Policy** page, select a provisioning policy option, and then click **Next** or **Finish**.

    The provisioning policy determines the ownership types available for accounts. The default provisioning policy enables only Individual ownership type accounts. Additional ownership types can be added by creating entitlements on the provisioning policy.

    Note: If you are creating a service for an identity feed, the **Configure Policy** page is not displayed.
13. Optional: On the **Reconcile Supporting Data** page, either do an immediate reconciliation for the service, or schedule a supporting data reconciliation, and then click **Finish**.

    The **Reconcile Supporting Data** page is displayed for all services except for identity feed services.

    The **supporting data only** reconciliation option retrieves only the supporting data for accounts. The supporting data includes groups that are defined on the service. The type of supporting data is defined in the adapter guide.
14. Optional: On the **Service Information** or **General Information** page, click **Test Connection** to validate that the data in the fields is correct, and then click **Next** or **Finish**.

    If the connection fails, contact the analyst who is responsible for the computer on which the managed resource runs.

Results

A message is displayed, indicating that you successfully created the service instance for a specific service type.

Related concepts

Installing the dispatcher
If this is the first Security Directory Integrator-based adapter installation, you must install the RMI Dispatcher before you install the adapter. Install the RMI Dispatcher on the same Security Directory Integrator server where you want to install the adapter.

Restarting the adapter service
Various installation and configuration tasks might require the adapter to be restarted to apply the changes. For example, you must restart the adapter if there are changes in the adapter profile, connector, or assembly lines. To restart the adapter, restart the Dispatcher.

Service/Target form details
Complete the service/target form fields.

Installing the adapter language package
The adapters use a separate language package from IBM Security Verify Identity.

Related tasks

Installing the adapter binaries or connector

The connector might or might not be available with the base Security Directory Integrator or Security Directory Integrator product. The connector is required to establish communication between the adapter and the Dispatcher.

Importing the adapter profile
An adapter profile defines the types of resources that the Identity server can manage. It is packaged with the IBM Security Verify Adapter. Use the adapter profile to create an adapter service on Identity server and establish communication with the adapter.

Verifying that the adapter is working correctly
After you install and configure the adapter, verify that the installation and configuration are correct.

Service/Target form details

Complete the service/target form fields.

Note: If the following fields on the service form are changed for an existing service, restart the IBM Security Verify Adapter service on the Security Directory Integrator server.

- **Directory Server Location**
- **Administrator Name**
- **Administrator Password**
- **Max Connection Count**
- **AL FileSystem Path**

On the LDAP service tab:

Service Name
Specify a name that defines the adapter service on the Identity server.

Note: Do not use forward (/) or backward slashes (\) in the service name.

Description
Optional: Specify a description that identifies the service for your environment.

Security Directory Integrator location

Specify the URL for the IBM Security Directory Integrator instance. The valid syntax for the URL is `rmi://`*`ip-address`*`:`*`port`*`/ITDIDispatcher`, where *ip-address* is the IBM Security Directory Integrator host and *port* is the port number for the RMI Dispatcher.

The default URL for the default SDI1 instance is `rmi://localhost:1099/ITDIDispatcher`.

URL
Specify the location and port number of the IBM Directory Server or Sun ONE Directory Server. Valid syntax is `ldap://ip-address:port`, where *ip-address* is the IBM Directory Server or Sun ONE Directory Server host and *port* is the IBM Directory Server or Sun ONE Directory Server port number. For example, you might specify the URL as `ldap://irvas02.eng.irvine.ibm.com:389`.

Use SSL communication with LDAP
Specify whether to use SSL-enabled communication between Security Directory Integrator and the managed LDAP resource. See “Enabling SSL communication” on page 41 for the steps to configure Security Directory Integrator for SSL-enabled communication with the LDAP resource.

Administrator name
Specify the user name for the administrator.

Password
Specify the password for the administrator name.

Directory server name
Specify the directory server type from the pull-down.

OpenLDAP returns a null value for the **`venderVersion`** attribute. The null value causes the entire Test Connection operation to fail.

Choosing the **Other** selection avoids the null value error because the adapter returns a string value of `Custom code needed` for the **venderVersion** attribute. Customizing the code is a requirement only if you want to provide a valid value for the **venderVersion** attribute. See "Customizing operations for the directory server" on page 28.

On the Users and Groups tab:

Users base DN
Specify the full distinguished name (DN) of the container or base point where the users are stored. The adapter creates new users under this DN. Also, search operations return user account entries under this DN. For example, you might specify the DN as ou=people,dc=com.

Users RDN
Specify the relative distinguished name (RDN) attribute for users' LDAP entries. The RDN is a static attribute for LDAP entries and must not be modified between operation.

Groups base DN
Specify the full distinguished name (DN) of the container or base point where the groups are stored. User membership, specified on the account form, refers to groups in this DN. Also, search operations return group entries under this DN. For example, you might specify the DN as ou=groups,dc=com.

Group RDN
Specify the relative distinguished name (RDN) attribute for the LDAP entries of the group. The RDN is a static attribute for LDAP entries and must not be modified between operation.

Initial Group Member
Specify the name of a user who can be a member of the group when you perform the group add operation. However, the user that you specify for this attribute might not exist on the managed resource. For example, you can specify the name of the user as `cn=TimAdapter`, where `TimAdapter` user might not exist on the managed resource.

Note: The user name that you specify must be in the DN format.

Group object class name
Specify the group object class name under which the group is added on the managed resource. You can select the group object class name from **groupOfNames** and **groupOfUniqueNames** object classes.

Group membership attribute
Specify the attribute of the group object class on the managed resource that list the users who are members of the group. You can select from **member** (groupOfNames object class) and **uniqueMember** (groupOfUniqueNames object class).

On the Dispatcher Attributes tab:

Disable AL Caching
Select the check box to disable the assembly line caching in the dispatcher for the service. The assembly lines for the add, modify, delete, and test operations are not cached.

AL FileSystem Path
Specify the file path from where the dispatcher loads the assembly lines. If you do not specify a file path, the dispatcher loads the assembly lines received from Identity server. For example, you can specify the following file path to load the assembly lines from the `profiles` directory of the Windows operating system: *drive*`:\Program Files\IBM\TDI\V7.1\profiles` or you can specify the following file path to load the assembly lines from the `profiles` directory of the UNIX and Linux® operating system: `/opt/IBM/TDI/V7.1/profiles`

Max Connection Count
Specify the maximum number of assembly lines that the dispatcher can execute simultaneously for the service. For example, enter `10` when you want the dispatcher to execute maximum ten assembly lines simultaneously for the service. If you enter `0` in the **Max Connection Count** field, the dispatcher does not limit the number of assembly lines that are executed simultaneously for the service.

On the Status and information tab

This page contains read only information about the adapter and managed resource. These fields are examples. The actual fields vary depending on the type of adapter and how the service form is configured. The adapter must be running to obtain the information. Click **Test Connection** to populate the fields.

Last status update: Date
Specifies the most recent date when the Status and information tab was updated.

Last status update: Time
Specifies the most recent time of the date when the Status and information tab was updated.

Managed resource status
Specifies the status of the managed resource that the adapter is connected to.

Adapter version
Specifies the version of the adapter that the IBM Security Verify Adapter service uses to provision request to the managed resource.

Profile version
Specifies the version of the profile that is installed in the Identity server.

TDI version
Specifies the version of the Security Directory Integrator on which the adapter is deployed.

Dispatcher version
Specifies the version of the Dispatcher.

Installation platform
Specifies summary information about the operating system where the adapter is installed.

Adapter account
Specifies the account that running the adapter binary file.

Adapter up time: Date
Specifies the date when the adapter started.

Adapter up time: Time
Specifies the time of the date when the adapter started.

Adapter memory usage
Specifies the memory usage for running the adapter.

If the connection fails, follow the instructions in the error message. Also

- Verify the adapter log to ensure that the test request was successfully sent to the adapter.
- Verify the adapter configuration information.
- Verify service parameters for the adapter profile. For example, verify the work station name or the IP address of the managed resource and the port.

Related concepts

Installing the dispatcher
If this is the first Security Directory Integrator-based adapter installation, you must install the RMI Dispatcher before you install the adapter. Install the RMI Dispatcher on the same Security Directory Integrator server where you want to install the adapter.

Restarting the adapter service
Various installation and configuration tasks might require the adapter to be restarted to apply the changes. For example, you must restart the adapter if there are changes in the adapter profile, connector, or assembly lines. To restart the adapter, restart the Dispatcher.

Installing the adapter language package
The adapters use a separate language package from IBM Security Verify Identity.

Related tasks

Installing the adapter binaries or connector

The connector might or might not be available with the base Security Directory Integrator or Security Directory Integrator product. The connector is required to establish communication between the adapter and the Dispatcher.

Importing the adapter profile
An adapter profile defines the types of resources that the Identity server can manage. It is packaged with the IBM Security Verify Adapter. Use the adapter profile to create an adapter service on Identity server and establish communication with the adapter.

Creating an adapter service/target
After you import the adapter profile on the Identity server, create a service/target so that Identity server can communicate with the managed resource.

Verifying that the adapter is working correctly
After you install and configure the adapter, verify that the installation and configuration are correct.

Installing the adapter language package

The adapters use a separate language package from IBM Security Verify Identity.

See *Installing the adapter language pack* from the IBM Security Verify Identity product documentation.

Related concepts

Installing the dispatcher
If this is the first Security Directory Integrator-based adapter installation, you must install the RMI Dispatcher before you install the adapter. Install the RMI Dispatcher on the same Security Directory Integrator server where you want to install the adapter.

Restarting the adapter service
Various installation and configuration tasks might require the adapter to be restarted to apply the changes. For example, you must restart the adapter if there are changes in the adapter profile, connector, or assembly lines. To restart the adapter, restart the Dispatcher.

Service/Target form details
Complete the service/target form fields.

Related tasks

Installing the adapter binaries or connector
The connector might or might not be available with the base Security Directory Integrator or Security Directory Integrator product. The connector is required to establish communication between the adapter and the Dispatcher.

Importing the adapter profile
An adapter profile defines the types of resources that the Identity server can manage. It is packaged with the IBM Security Verify Adapter. Use the adapter profile to create an adapter service on Identity server and establish communication with the adapter.

Creating an adapter service/target
After you import the adapter profile on the Identity server, create a service/target so that Identity server can communicate with the managed resource.

Verifying that the adapter is working correctly
After you install and configure the adapter, verify that the installation and configuration are correct.

Verifying that the adapter is working correctly

After you install and configure the adapter, verify that the installation and configuration are correct.

Procedure

1. Test the connection for the service that you created on the Identity server.
2. Run a full reconciliation from the Identity server.
3. Run all supported operations such as add, modify, and delete on one user account.

4. Verify the `ibmdi.log` file after each operation to ensure that no errors are reported.
5. Verify the `trace.log` file to ensure that no errors are reported when you run an adapter operation.

Related concepts

Installing the dispatcher
If this is the first Security Directory Integrator-based adapter installation, you must install the RMI Dispatcher before you install the adapter. Install the RMI Dispatcher on the same Security Directory Integrator server where you want to install the adapter.

Restarting the adapter service
Various installation and configuration tasks might require the adapter to be restarted to apply the changes. For example, you must restart the adapter if there are changes in the adapter profile, connector, or assembly lines. To restart the adapter, restart the Dispatcher.

Service/Target form details
Complete the service/target form fields.

Installing the adapter language package
The adapters use a separate language package from IBM Security Verify Identity.

Related tasks

Installing the adapter binaries or connector
The connector might or might not be available with the base Security Directory Integrator or Security Directory Integrator product. The connector is required to establish communication between the adapter and the Dispatcher.

Importing the adapter profile
An adapter profile defines the types of resources that the Identity server can manage. It is packaged with the IBM Security Verify Adapter. Use the adapter profile to create an adapter service on Identity server and establish communication with the adapter.

Creating an adapter service/target
After you import the adapter profile on the Identity server, create a service/target so that Identity server can communicate with the managed resource.

Chapter 4. Upgrading

Upgrading an IBM Security Directory Integrator-based adapter involves tasks such as upgrading the dispatcher, the connector, and the adapter profile. Depending on the adapter, some of these tasks might not be applicable. Other tasks might also be required to complete the upgrade.

To verify the required version of these adapter components, see the adapter release notes. For the installation steps, see Chapter 3, “Installing,” on page 11.

Upgrading the adapter profile

Read the adapter release notes for any specific instructions before you import a new adapter profile on IBM Security Verify Identity.

See Importing the adapter profile.

Note: Restart the dispatcher service after importing the profile. Restarting the dispatcher clears the assembly lines cache and ensures that the dispatcher runs the assembly lines from the updated adapter profile.

Chapter 5. Configuring

After you install the adapter, configure it to function correctly. Configuration is based on your requirements or preference.

See the *IBM Security Dispatcher Installation and Configuration Guide* for additional configuration options such as:

- JVM properties
- Dispatcher filtering
- Dispatcher properties
- Dispatcher port number
- Logging configurations
- Secure Sockets Layer (SSL) communication

For more information about deploying and customizing the adapter, see the customization white paper entitled *IBM Security Verify Identity, Version 6.0 Customization and Deployment Guide for the LDAP Adapter*.

The adapter is designed to work with the inetOrgPerson object class, a general-purpose object class that contains attributes about people. If you are using the inetOrgPerson schema for your directory, the LDAP Adapter does not require customization. If your directory uses the UID attribute as the relative distinguished name (RDN), do not customize the adapter. The UID attribute must be the first component of the DN. For example, UID=Test User, ou=Accounting.

The adapter is designed to work with the groupOfNames and groupOfUniqueNames object classes, a general-purpose object class that contains attributes about groups. If you are using the groupOfNames and groupOfUniqueNames schema for your directory, the LDAP Adapter does not require customization.

The adapter supports a standard set of attributes and object classes for a directory server. The adapter supports standard user provisioning operations such as add, delete, modify, suspend, restore, change password, search, and test. The adapter also supports group operations, such as add, modify, and delete. The directory server requirements vary. Therefore, you might customize or extend the LDAP schema to support additional attributes or object classes.

Customizing the adapter profile

To customize the adapter profile, you must modify the LDAP Adapter JAR file, `LdapProfile.jar`.

About this task

You might customize the adapter profile to change the account form or the service form.

The `LdapProfile.jar` file is included in the LDAP Adapter compressed file that you downloaded from the IBM website. The JAR file contains the following files:

- CustomLabels.properties
- erLDAPAccount.xml
- erLDAPRMIService.xml
- service.def
- schema.dsml
- LdapAL.xml
- LDAPAdd.xml
- LDAPDelete.xml
- LDAPModify.xml

- LDAPTest.xml
- erLDAPGroupAccount.xml
- LDAPGroupAdd.xml
- LDAPGroupModify.xml
- LDAPGroupDelete.xml

For more information about customizing the adapter profile, see the *IBM Security Verify Identity, Version 6.0 Customization and Deployment Guide for the LDAP Adapter* white paper.

To edit and import the adapter profile, take these steps:

Procedure

- To edit the `LdapProfile.jar` file, complete these steps:
  a) Log on to the workstation where the IBM Directory Server or Sun ONE Directory Server is installed.
  b) On the **Start** menu, click **Programs** → **Accessories** → **Command Prompt**.
  c) Copy the JAR file into a temporary directory.
  d) Extract the contents of the JAR file into the temporary directory by running the following command. The following example applies to the LDAP Adapter profile. Type the name of the JAR file for your operating system.

```
cd c:\temp
jar -xvf LdapProfile.jar
```

  The **jar** command extracts the files into the directory.
  e) Edit the file that you want to change.
- After you edit the file, you must import the file into the Identity server for the changes to take effect. To import the file, perform these steps:
  a) Create a JAR file with the files in the `\temp` directory by running the following commands:

```
cd c:\temp  jar -cvfLdapProfile.jar LdapProfile
```

  b) Import the JAR file into the IBM Security Verify Identity application server.
  c) Stop and start the Identity server
  d) Restart the adapter service.

Editing adapter profiles on the UNIX or Linux operating system

The adapter profile `.jar` file might contain ASCII files that are created by using the MS-DOS ASCII format.

About this task

If you edit an MS-DOS ASCII file on the UNIX operating system, you might see a character `^M` at the end of each line. These characters indicate new lines of text in MS-DOS. The characters can interfere with the running of the file on UNIX or Linux systems. You can use tools, such as **dos2unix**, to remove the `^M` characters. You can also use text editors, such as the **vi** editor, to remove the characters manually.

Example

You can use the **vi** editor to remove the `^M` characters. From the **vi** command mode, run the following command and press Enter:

```
:%s/^M//g
```

When you use this command, enter ^M or Ctrl-M by pressing **^v^M** or **Ctrl V Ctrl M** sequentially. The **^v** instructs the **vi** editor to use the next keystroke instead of issuing it as a command.

Standard parameters

The LDAP Adapter is configured to use a standard set of parameters. The LDAP resource must support referential integrity.

inetOrgPerson
The default object class used to create new users. The supporting object classes are **organizationalPerson**, **person**, and **top**.

groupOfNames or groupOfUniqueNames
The adapter supports these object classes to assign users to groups and create new groups.

Standard attributes

After you install the adapter profile, the LDAP Adapter supports a standard set of attributes.

Table 3 on page 27 lists the standard inetOrgPerson attributes supported by the LDAP Adapter.

Table 3. Attributes supported by the LDAP Adapter

businessCategory	homePostalAddress	preferredLanguage
carLicense	initials	registeredAddress
cn	l	roomNumber
departmentNumber	mail	secretary
description	manager	sn
destinationIndicator	mobile	st
displayName	pager	street
employeeNumber	physicalDeliveryOfficeName	telephoneNumber
employeeType	postalAddress	teletexTerminalIdentifier
facisimileTelephoneNumber	postalCode	telexNumber
givenName	postOfficeBox	title
homePhone	preferreddeliverymethod	userPassword

Table 4 on page 27 lists the standard groupOfNames and groupOfUniqueNames attributes supported by the LDAP Adapter.

Table 4. Attributes supported by the LDAP Adapter

Attribute	Description
erldapservicegroup	Specifies the name of the group.
erldapgroupdescription	Specifies a brief description about the group.
erldapgroupfullname	Specifies full name of the group.
erldapgroupowner	Specifies the owner of the group.
erldapgroupbusinesscategory	Specifies the group business category.
erldapgrouporganization	Specifies the group organization.
erldapgrouporganizationalunit	Specifies the group organizational unit.

Table 4. Attributes supported by the LDAP Adapter (continued)	
Attribute	**Description**
erldapgroupseealso	See Also.

Customizing operations for the directory server

Use these customized operations for either IBM Directory Server or Sun ONE Directory Server. If you use a different directory server, you must customize these operations for your server.

If a directory server other than IBM Directory Server or Sun ONE Directory Server is used to manage resources, the suspend, restore, and search operations must be customized. Complete these tasks to customize the above operations for a different directory server.

User account suspension

You can use the default customization for the suspend operation for either IBM Directory Server or Sun ONE Directory Server.

If you use a different directory server, you might need to change the default customization for this operation.

`userPassword`
For IBM Security Directory Server, the **`userPassword`** attribute is deleted to disable a user account.

`nsaccountlock`
For Sun Java System Directory Server, the **`nsaccountlock`** attribute is used to suspend a user account. The default value is `True`.

Note: The adapter returns warning, if the user is already suspended.

Related concepts

User account restoration
You can use the default customization for the restore operation for either IBM Directory Server or Sun ONE Directory Server.

User account searches
You can use the default customization for the search operation for either IBM Directory Server or Sun ONE Directory Server. If you use a different directory server, you must change the default customization for this operation.

The CN attribute as the ldapUserRDN
The adapter maps the value of the LDAP **`CN`** attribute to the **`ERUID`** and **`CN`** attributes of the Identity server. The number of values for the LDAP **`CN`** attributes affects the mapping.

pwdChangeTime attribute for the LDAP Adapter
When a password policy is enabled, the **`pwdChangedTime`** attribute is set on the resource for each person or user entry when the password is changed by an administrator.

Commas in the cn attribute
If you use commas in the **`cn`** attribute, the following guidelines apply:

Support for the pwdReset attribute
When password policy is enabled, the **`pwdReset`** attribute is set on the resource for each person or user entry when the password is changed by an administrator.

RDN attribute change for the group account
To change the RDN attribute for a group account, change these files to map the **`cn`** attribute to the required RDN attribute:

Base point configuration
The base point for the LDAP Adapter is the point in the directory server that is used as the root for the adapter. The base point can be an organizational unit (OU) or domain container (DC) base point.

Support for ibm-slapdSetenv: IBMLDAP_ATTR_INCLUDE_BINARY property

See this topic for more information about the support for the `ibm-slapdSetenv: IBMLDAP_ATTR_INCLUDE_BINARY` property in IBM Security Directory Server, version 6.3.1 and later.

Related tasks

Adding support for a new user/group object class
You can add support for a new user/group object class.

Adding support for a new directory server
You can add support for a new directory server.

User account restoration

You can use the default customization for the restore operation for either IBM Directory Server or Sun ONE Directory Server.

If you use a different directory server, you might need to change the default customization for this operation.

`userPassword`
For IBM Security Directory Server, the **`userPassword`** attribute is used to set the password for a user.

`nsaccountlock`
For Sun Java System Directory Server, the **`nsaccountlock`** attribute is used to restore a user account. The default value is `False`.

Note: The adapter returns warning, if the user is already restored.

Related concepts

User account suspension
You can use the default customization for the suspend operation for either IBM Directory Server or Sun ONE Directory Server.

User account searches
You can use the default customization for the search operation for either IBM Directory Server or Sun ONE Directory Server. If you use a different directory server, you must change the default customization for this operation.

The CN attribute as the ldapUserRDN
The adapter maps the value of the LDAP **`CN`** attribute to the **`ERUID`** and **`CN`** attributes of the Identity server. The number of values for the LDAP **`CN`** attributes affects the mapping.

pwdChangeTime attribute for the LDAP Adapter
When a password policy is enabled, the **`pwdChangedTime`** attribute is set on the resource for each person or user entry when the password is changed by an administrator.

Commas in the cn attribute
If you use commas in the **`cn`** attribute, the following guidelines apply:

Support for the pwdReset attribute
When password policy is enabled, the **`pwdReset`** attribute is set on the resource for each person or user entry when the password is changed by an administrator.

RDN attribute change for the group account
To change the RDN attribute for a group account, change these files to map the **`cn`** attribute to the required RDN attribute:

Base point configuration
The base point for the LDAP Adapter is the point in the directory server that is used as the root for the adapter. The base point can be an organizational unit (OU) or domain container (DC) base point.

Support for ibm-slapdSetenv: IBMLDAP_ATTR_INCLUDE_BINARY property
See this topic for more information about the support for the `ibm-slapdSetenv: IBMLDAP_ATTR_INCLUDE_BINARY` property in IBM Security Directory Server, version 6.3.1 and later.

Related tasks

Adding support for a new user/group object class

You can add support for a new user/group object class.

Adding support for a new directory server
You can add support for a new directory server.

User account searches

You can use the default customization for the search operation for either IBM Directory Server or Sun ONE Directory Server. If you use a different directory server, you must change the default customization for this operation.

userPassword
For IBM Security Directory Server, the status of the account is based on the userPassword attribute. When a search is performed, if userPassword is mapped to erAccountStatus, the account is active and the value of erAccountStatus is 0. If userPassword is not mapped to erAccountStatus, the account is suspended and the value of erAccountStatus is 1.

nsaccountlock
For Sun Java System Directory Server, the status of an account is based on the nsaccountlock attribute. When a search is performed, if nsaccountlock is set to true, the account is disabled and the value of erAccountStatus is 1. If nsaccountlock is set to false, the account is enabled and the value of erAccountStatus is 0.

Related concepts

User account suspension
You can use the default customization for the suspend operation for either IBM Directory Server or Sun ONE Directory Server.

User account restoration
You can use the default customization for the restore operation for either IBM Directory Server or Sun ONE Directory Server.

The CN attribute as the ldapUserRDN
The adapter maps the value of the LDAP **CN** attribute to the **ERUID** and **CN** attributes of the Identity server. The number of values for the LDAP **CN** attributes affects the mapping.

pwdChangeTime attribute for the LDAP Adapter
When a password policy is enabled, the **pwdChangedTime** attribute is set on the resource for each person or user entry when the password is changed by an administrator.

Commas in the cn attribute
If you use commas in the **cn** attribute, the following guidelines apply:

Support for the pwdReset attribute
When password policy is enabled, the **pwdReset** attribute is set on the resource for each person or user entry when the password is changed by an administrator.

RDN attribute change for the group account
To change the RDN attribute for a group account, change these files to map the **cn** attribute to the required RDN attribute:

Base point configuration
The base point for the LDAP Adapter is the point in the directory server that is used as the root for the adapter. The base point can be an organizational unit (OU) or domain container (DC) base point.

Support for ibm-slapdSetenv: IBMLDAP_ATTR_INCLUDE_BINARY property
See this topic for more information about the support for the `ibm-slapdSetenv: IBMLDAP_ATTR_INCLUDE_BINARY` property in IBM Security Directory Server, version 6.3.1 and later.

Related tasks

Adding support for a new user/group object class
You can add support for a new user/group object class.

Adding support for a new directory server

You can add support for a new directory server.

The CN attribute as the ldapUserRDN

The adapter maps the value of the LDAP **CN** attribute to the **ERUID** and **CN** attributes of the Identity server. The number of values for the LDAP **CN** attributes affects the mapping.

If there is only one value for the **CN** attribute on resource, the adapter maps it to both:

- The **ERUID** attribute
- The **CN** attribute of the **Account Object Class**.

For example, if the following is an entry on the LDAP resource:

```
Dn: cn=tuser3,ou=users,dc=com
objectclass: inetorgperson; organizationalperson; person; top;
sn: tuser3sn;
cn: tuser3;
```

The adapter maps `tuser3` to the **ERUID** and **CN** attributes. The entry stored in LDAP is:

```
Dn:
erglobalid=9113975423632247385,ou=orphans,
erglobalid=00000000000000000000,ou=ibm,dc=com
eruid: tuser3;
ercreatedate: 201006281214Z;
sn: tuser3sn;
erparent:
erglobalid=9113850732946037237,ou=services,
erglobalid=00000000000000000000,ou=ibm,dc=com;
objectclass: top; erLDAPUserAccount; erManagedItem; inetorgperson;
organizationalPerson; person; erAccountItem;
erglobalid: 9113975423632247385;
cn: tuser3;
eraccountstatus: 0;
erservice: erglobalid=9113850732946037237,ou=services,
erglobalid=00000000000000000000,ou=ibm,dc=com;
erldapcontainername: ou=users,dc=com;
```

More than one value can exist on the resource for the **CN** attribute. If **CN** is used as the **User RDN** attribute on service form, the adapter maps one value of **CN** to the **ERUID** attribute. This value is the one used as the RDN value in the **DN** attribute on resource LDAP. The adapter maps the rest of the values to the **CN** attribute.

For example, if following is an entry on resource LDAP:

```
Dn: cn=user5,ou=users,dc=com
objectclass: inetorgperson; organizationalPerson; person; top;
sn: snval1; snval2;
cn: cnval2; cnval3; user5;
```

The adapter maps `user5` to the **ERUID** attribute and all other values to the **CN** attribute. The entry stored in LDAP is:

```
Dn: erglobalid=9113975423903405991,ou=orphans,
erglobalid=00000000000000000000,ou=ibm,dc=com
eruid: user5;
ercreatedate: 201006281214Z;
sn: snval1; snval2;
erparent: erglobalid=9113850732946037237,ou=services,
erglobalid=00000000000000000000,ou=ibm,dc=com;
objectclass: top; erLDAPUserAccount; erManagedItem; inetorgperson;
organizationalPerson; person; erAccountItem;
erglobalid: 9113975423903405991;
cn: cnval2; cnval3;
eraccountstatus: 1;
erservice: erglobalid=9113850732946037237,ou=services,
erglobalid=00000000000000000000,ou=ibm,dc=com;
erldapcontainername: ou=users,dc=com;
```

Related concepts

User account suspension
You can use the default customization for the suspend operation for either IBM Directory Server or Sun ONE Directory Server.

User account restoration
You can use the default customization for the restore operation for either IBM Directory Server or Sun ONE Directory Server.

User account searches
You can use the default customization for the search operation for either IBM Directory Server or Sun ONE Directory Server. If you use a different directory server, you must change the default customization for this operation.

pwdChangeTime attribute for the LDAP Adapter
When a password policy is enabled, the **pwdChangedTime** attribute is set on the resource for each person or user entry when the password is changed by an administrator.

Commas in the cn attribute
If you use commas in the **cn** attribute, the following guidelines apply:

Support for the pwdReset attribute
When password policy is enabled, the **pwdReset** attribute is set on the resource for each person or user entry when the password is changed by an administrator.

RDN attribute change for the group account
To change the RDN attribute for a group account, change these files to map the **cn** attribute to the required RDN attribute:

Base point configuration
The base point for the LDAP Adapter is the point in the directory server that is used as the root for the adapter. The base point can be an organizational unit (OU) or domain container (DC) base point.

Support for ibm-slapdSetenv: IBMLDAP_ATTR_INCLUDE_BINARY property
See this topic for more information about the support for the `ibm-slapdSetenv: IBMLDAP_ATTR_INCLUDE_BINARY` property in IBM Security Directory Server, version 6.3.1 and later.

Related tasks

Adding support for a new user/group object class
You can add support for a new user/group object class.

Adding support for a new directory server
You can add support for a new directory server.

pwdChangeTime attribute for the LDAP Adapter

When a password policy is enabled, the **pwdChangedTime** attribute is set on the resource for each person or user entry when the password is changed by an administrator.

The value for this attribute is in Coordinated Universal Time (UTC) format. The attribute is on the account form with the label **Last Password Changed TimeStamp**. The **pwdChangedTime** attribute is a read/write attribute in Security Directory Server version 6.2. You can modify the value of the **pwdChangedTime** attribute in Security Directory Server only if both of these conditions are met:

- A password policy is enabled.
- The **Password policy enabled on directory server** check box on the service form is selected.

Note: If **Password policy enabled on directory server** is checked on the service form, the following behaviors occur for Security Directory Server version 6.2 only:

Add operation
When a new user account is requested with a value specified for the **Last Password Changed Timestamp** fields on the Account Form, adapter does not set the value for **pwdChangedTime** attribute on the resource. It returns a warning message `pwdChangedTime attribute not supported during add operation.`

Modify operation
The values specified for the **Last Password Changed Timestamp** fields on the account form are set on the resource. This action applies to Security Directory Server with password policy enabled only.

Reconciliation operation
Adapter reconciles the value of the **pwdChangedTime** attribute for each account. This action occurs regardless of the value specified for **Password policy enabled on directory server?**.

The value for the **pwdChangedTime** attribute is changed on Security Directory Server to prevent the password for a particular account from expiring. When setting the **userPassword** attribute set the **pwdChangedTime** attribute to a future date. The following example sets the time to midnight, January 1, 2200.

```
Ldapmodify -D cn=root -w ? -k
dn:uid=wasadmin,cn=users,o=ibm
changetype:modify
replace:pwdChangedTime
pwdChangedTime:22000101000000Z
```

In Sun One Directory Server version 6.3 the **pwdChangedTime** attribute is read only. To modify this attribute for each person and user entry on the managed resource:

- Set the **usePwdChangedTime** attribute to 0N.
- Manually set this attribute on the resource, in the schema section under `cn=config`.

Note: The adapter reconciles the value of the **pwdChangedTime** attribute for Sun One Directory Server.

Related concepts

User account suspension
You can use the default customization for the suspend operation for either IBM Directory Server or Sun ONE Directory Server.

User account restoration
You can use the default customization for the restore operation for either IBM Directory Server or Sun ONE Directory Server.

User account searches
You can use the default customization for the search operation for either IBM Directory Server or Sun ONE Directory Server. If you use a different directory server, you must change the default customization for this operation.

The CN attribute as the ldapUserRDN
The adapter maps the value of the LDAP **CN** attribute to the **ERUID** and **CN** attributes of the Identity server. The number of values for the LDAP **CN** attributes affects the mapping.

Commas in the cn attribute
If you use commas in the **cn** attribute, the following guidelines apply:

Support for the pwdReset attribute
When password policy is enabled, the **pwdReset** attribute is set on the resource for each person or user entry when the password is changed by an administrator.

RDN attribute change for the group account
To change the RDN attribute for a group account, change these files to map the **cn** attribute to the required RDN attribute:

Base point configuration
The base point for the LDAP Adapter is the point in the directory server that is used as the root for the adapter. The base point can be an organizational unit (OU) or domain container (DC) base point.

Support for ibm-slapdSetenv: IBMLDAP_ATTR_INCLUDE_BINARY property
See this topic for more information about the support for the `ibm-slapdSetenv: IBMLDAP_ATTR_INCLUDE_BINARY` property in IBM Security Directory Server, version 6.3.1 and later.

Related tasks

Adding support for a new user/group object class

You can add support for a new user/group object class.

Adding support for a new directory server
You can add support for a new directory server.

Commas in the cn attribute

If you use commas in the **cn** attribute, the following guidelines apply:

- Do not provide a backward slash (\) before a comma on the account form.
- If the **User base DN** is `ou=users,dc=com`, but on the resource it is `cn=abc\,xyz, ou=users,dc=com`, the entry is created. However, the value of the **cn** attribute remains `abc,xyz` on the LDAP resource.
- Filtered reconciliation requires that The filter query must be in the form `eruid=abc,xyz`.

Related concepts

User account suspension
You can use the default customization for the suspend operation for either IBM Directory Server or Sun ONE Directory Server.

User account restoration
You can use the default customization for the restore operation for either IBM Directory Server or Sun ONE Directory Server.

User account searches
You can use the default customization for the search operation for either IBM Directory Server or Sun ONE Directory Server. If you use a different directory server, you must change the default customization for this operation.

The CN attribute as the ldapUserRDN
The adapter maps the value of the LDAP **CN** attribute to the **ERUID** and **CN** attributes of the Identity server. The number of values for the LDAP **CN** attributes affects the mapping.

pwdChangeTime attribute for the LDAP Adapter
When a password policy is enabled, the **pwdChangedTime** attribute is set on the resource for each person or user entry when the password is changed by an administrator.

Support for the pwdReset attribute
When password policy is enabled, the **pwdReset** attribute is set on the resource for each person or user entry when the password is changed by an administrator.

RDN attribute change for the group account
To change the RDN attribute for a group account, change these files to map the **cn** attribute to the required RDN attribute:

Base point configuration
The base point for the LDAP Adapter is the point in the directory server that is used as the root for the adapter. The base point can be an organizational unit (OU) or domain container (DC) base point.

Support for ibm-slapdSetenv: IBMLDAP_ATTR_INCLUDE_BINARY property
See this topic for more information about the support for the `ibm-slapdSetenv: IBMLDAP_ATTR_INCLUDE_BINARY` property in IBM Security Directory Server, version 6.3.1 and later.

Related tasks

Adding support for a new user/group object class
You can add support for a new user/group object class.

Adding support for a new directory server

You can add support for a new directory server.

Support for the pwdReset attribute

When password policy is enabled, the **pwdReset** attribute is set on the resource for each person or user entry when the password is changed by an administrator.

To use the **pwdReset** attribute, the **Password policy enabled on directory server** option on the service form must be checked.

The **pwdReset** attribute is on the account form with a label **Force a password change at next logon?**. The adapter can configure this attribute. When this field is checked on the account form, adapter sets the value of **pwdReset** attribute to TRUE on the resource. If unchecked on the account form, the adapter sets the value to FALSE.

Note: The **pwdReset** attribute is not supported for Sun Directory Server.

If **Password policy enabled on directory server** is checked on the service form, the following behaviors occur:

Add operation
When a new user account is requested with a value specified for the **Force a password change at next logon?** field on the account form, adapter sets the value for **pwdReset** attribute on resource. If checked, the value is set to TRUE. If unchecked, the value is set to FALSE.

Modify operation
The value specified for the **Force a password change at next logon?** field on the account form is set on the resource.

Password change operation
The value specified for the **Force a password change at next logon?** field on the account form is set on the resource.

Suspend operation
The adapter does not set the value of the **pwdReset** attribute.

Restore operation
The value specified for the **Force a password change at next logon?** field on the account form is set on the resource.

Reconciliation operation
Adapter reconciles the value of the **pwdRest** attribute for each account. This action occurs regardless of the value specified for **Password policy enabled on directory server?**.

Related concepts

User account suspension
You can use the default customization for the suspend operation for either IBM Directory Server or Sun ONE Directory Server.

User account restoration
You can use the default customization for the restore operation for either IBM Directory Server or Sun ONE Directory Server.

User account searches
You can use the default customization for the search operation for either IBM Directory Server or Sun ONE Directory Server. If you use a different directory server, you must change the default customization for this operation.

The CN attribute as the ldapUserRDN
The adapter maps the value of the LDAP **CN** attribute to the **ERUID** and **CN** attributes of the Identity server. The number of values for the LDAP **CN** attributes affects the mapping.

pwdChangeTime attribute for the LDAP Adapter
When a password policy is enabled, the **pwdChangedTime** attribute is set on the resource for each person or user entry when the password is changed by an administrator.

Commas in the cn attribute

If you use commas in the **cn** attribute, the following guidelines apply:

RDN attribute change for the group account
To change the RDN attribute for a group account, change these files to map the **cn** attribute to the required RDN attribute:

Base point configuration
The base point for the LDAP Adapter is the point in the directory server that is used as the root for the adapter. The base point can be an organizational unit (OU) or domain container (DC) base point.

Support for ibm-slapdSetenv: IBMLDAP_ATTR_INCLUDE_BINARY property
See this topic for more information about the support for the `ibm-slapdSetenv: IBMLDAP_ATTR_INCLUDE_BINARY` property in IBM Security Directory Server, version 6.3.1 and later.

Related tasks
Adding support for a new user/group object class
You can add support for a new user/group object class.

Adding support for a new directory server
You can add support for a new directory server.

RDN attribute change for the group account

To change the RDN attribute for a group account, change these files to map the **cn** attribute to the required RDN attribute:

- LDAPAdd.xml
- LDAPDelete.xml
- LDAPModify.xml
- LDAPSearch.xml
- LDAPGroupAdd.xml
- LDAPGroupModify.xml
- LDAPGroupDelete.xml

Related concepts
User account suspension
You can use the default customization for the suspend operation for either IBM Directory Server or Sun ONE Directory Server.

User account restoration
You can use the default customization for the restore operation for either IBM Directory Server or Sun ONE Directory Server.

User account searches
You can use the default customization for the search operation for either IBM Directory Server or Sun ONE Directory Server. If you use a different directory server, you must change the default customization for this operation.

The CN attribute as the ldapUserRDN
The adapter maps the value of the LDAP **CN** attribute to the **ERUID** and **CN** attributes of the Identity server. The number of values for the LDAP **CN** attributes affects the mapping.

pwdChangeTime attribute for the LDAP Adapter
When a password policy is enabled, the **pwdChangedTime** attribute is set on the resource for each person or user entry when the password is changed by an administrator.

Commas in the cn attribute
If you use commas in the **cn** attribute, the following guidelines apply:

Support for the pwdReset attribute

When password policy is enabled, the **pwdReset** attribute is set on the resource for each person or user entry when the password is changed by an administrator.

Base point configuration
The base point for the LDAP Adapter is the point in the directory server that is used as the root for the adapter. The base point can be an organizational unit (OU) or domain container (DC) base point.

Support for ibm-slapdSetenv: IBMLDAP_ATTR_INCLUDE_BINARY property
See this topic for more information about the support for the `ibm-slapdSetenv: IBMLDAP_ATTR_INCLUDE_BINARY` property in IBM Security Directory Server, version 6.3.1 and later.

Related tasks

Adding support for a new user/group object class
You can add support for a new user/group object class.

Adding support for a new directory server
You can add support for a new directory server.

Adding support for a new user/group object class

You can add support for a new user/group object class.

Procedure

1. Change the schema.dsml file to use the new user/group object class.
2. Change the service.def file to use the new user/group object class.
3. Change the customLabels.properties file to synchronize the previous steps.
4. Change these files to use the new object classes:
   - LDAPAdd.xml
   - LDAPDelete.xml
   - LDAPModify.xml
   - LDAPSearch.xml
   - LDAPGroupAdd.xml
   - LDAPGroupModify.xml
   - LDAPGroupDelete.xml

Related concepts

User account suspension
You can use the default customization for the suspend operation for either IBM Directory Server or Sun ONE Directory Server.

User account restoration
You can use the default customization for the restore operation for either IBM Directory Server or Sun ONE Directory Server.

User account searches
You can use the default customization for the search operation for either IBM Directory Server or Sun ONE Directory Server. If you use a different directory server, you must change the default customization for this operation.

The CN attribute as the ldapUserRDN
The adapter maps the value of the LDAP **CN** attribute to the **ERUID** and **CN** attributes of the Identity server. The number of values for the LDAP **CN** attributes affects the mapping.

pwdChangeTime attribute for the LDAP Adapter
When a password policy is enabled, the **pwdChangedTime** attribute is set on the resource for each person or user entry when the password is changed by an administrator.

Commas in the cn attribute

If you use commas in the **cn** attribute, the following guidelines apply:

Support for the pwdReset attribute
When password policy is enabled, the **pwdReset** attribute is set on the resource for each person or user entry when the password is changed by an administrator.

RDN attribute change for the group account
To change the RDN attribute for a group account, change these files to map the **cn** attribute to the required RDN attribute:

Base point configuration
The base point for the LDAP Adapter is the point in the directory server that is used as the root for the adapter. The base point can be an organizational unit (OU) or domain container (DC) base point.

Support for ibm-slapdSetenv: IBMLDAP_ATTR_INCLUDE_BINARY property
See this topic for more information about the support for the `ibm-slapdSetenv: IBMLDAP_ATTR_INCLUDE_BINARY` property in IBM Security Directory Server, version 6.3.1 and later.

Related tasks

Adding support for a new directory server
You can add support for a new directory server.

Base point configuration

The base point for the LDAP Adapter is the point in the directory server that is used as the root for the adapter. The base point can be an organizational unit (OU) or domain container (DC) base point.

To configure the base point, specify the appropriate base point (User or Group) when you create or change a service using the adapter service form.

Related concepts

User account suspension
You can use the default customization for the suspend operation for either IBM Directory Server or Sun ONE Directory Server.

User account restoration
You can use the default customization for the restore operation for either IBM Directory Server or Sun ONE Directory Server.

User account searches
You can use the default customization for the search operation for either IBM Directory Server or Sun ONE Directory Server. If you use a different directory server, you must change the default customization for this operation.

The CN attribute as the ldapUserRDN
The adapter maps the value of the LDAP **CN** attribute to the **ERUID** and **CN** attributes of the Identity server. The number of values for the LDAP **CN** attributes affects the mapping.

pwdChangeTime attribute for the LDAP Adapter
When a password policy is enabled, the **pwdChangedTime** attribute is set on the resource for each person or user entry when the password is changed by an administrator.

Commas in the cn attribute
If you use commas in the **cn** attribute, the following guidelines apply:

Support for the pwdReset attribute
When password policy is enabled, the **pwdReset** attribute is set on the resource for each person or user entry when the password is changed by an administrator.

RDN attribute change for the group account
To change the RDN attribute for a group account, change these files to map the **cn** attribute to the required RDN attribute:

Support for ibm-slapdSetenv: IBMLDAP_ATTR_INCLUDE_BINARY property

See this topic for more information about the support for the `ibm-slapdSetenv: IBMLDAP_ATTR_INCLUDE_BINARY` property in IBM Security Directory Server, version 6.3.1 and later.

Related tasks

Adding support for a new user/group object class
You can add support for a new user/group object class.

Adding support for a new directory server
You can add support for a new directory server.

Adding support for a new directory server

You can add support for a new directory server.

Procedure

1. Change the erLDAPRMIService.xml file to allow the directory server drop-down menu to include the new server.
2. Change the `schema.dsml` file to use the new user/group object class.
3. Change the `service.def` file to use the new user/group object class.
4. Change the `customLabels.properties` file to synchronize the previous steps.
5. Change these files to use the new object classes and the new directory server:
   - LDAPAdd.xml
   - LDAPDelete.xml
   - LDAPModify.xml
   - LDAPSearch.xml

Related concepts

User account suspension
You can use the default customization for the suspend operation for either IBM Directory Server or Sun ONE Directory Server.

User account restoration
You can use the default customization for the restore operation for either IBM Directory Server or Sun ONE Directory Server.

User account searches
You can use the default customization for the search operation for either IBM Directory Server or Sun ONE Directory Server. If you use a different directory server, you must change the default customization for this operation.

The CN attribute as the ldapUserRDN
The adapter maps the value of the LDAP **CN** attribute to the **ERUID** and **CN** attributes of the Identity server. The number of values for the LDAP **CN** attributes affects the mapping.

pwdChangeTime attribute for the LDAP Adapter
When a password policy is enabled, the **pwdChangedTime** attribute is set on the resource for each person or user entry when the password is changed by an administrator.

Commas in the cn attribute
If you use commas in the **cn** attribute, the following guidelines apply:

Support for the pwdReset attribute
When password policy is enabled, the **pwdReset** attribute is set on the resource for each person or user entry when the password is changed by an administrator.

RDN attribute change for the group account
To change the RDN attribute for a group account, change these files to map the **cn** attribute to the required RDN attribute:

Base point configuration

The base point for the LDAP Adapter is the point in the directory server that is used as the root for the adapter. The base point can be an organizational unit (OU) or domain container (DC) base point.

Support for ibm-slapdSetenv: IBMLDAP_ATTR_INCLUDE_BINARY property
See this topic for more information about the support for the `ibm-slapdSetenv: IBMLDAP_ATTR_INCLUDE_BINARY` property in IBM Security Directory Server, version 6.3.1 and later.

Related tasks

Adding support for a new user/group object class
You can add support for a new user/group object class.

Support for ibm-slapdSetenv: IBMLDAP_ATTR_INCLUDE_BINARY property

See this topic for more information about the support for the `ibm-slapdSetenv: IBMLDAP_ATTR_INCLUDE_BINARY` property in IBM Security Directory Server, version 6.3.1 and later.

If the environment variable `IBMLDAP_ATTR_INCLUDE_BINARY` is set to `FALSE` or `NO` in the server startup environment or the `cn=Front End` entry of the `ibmslapd.conf file` is `ibm-slapdSetenv: IBMLDAP_ATTR_INCLUDE_BINARY=FALSE`, the server does not add the `;binary` tag to the binary attribute names unless they are explicitly specified by the client.

During the reconciliation operation, the `;binary` tag check is added in the code.

For the Modify operations, the attribute `userPassword;binary` is added to the map.

Related concepts

User account suspension
You can use the default customization for the suspend operation for either IBM Directory Server or Sun ONE Directory Server.

User account restoration
You can use the default customization for the restore operation for either IBM Directory Server or Sun ONE Directory Server.

User account searches
You can use the default customization for the search operation for either IBM Directory Server or Sun ONE Directory Server. If you use a different directory server, you must change the default customization for this operation.

The CN attribute as the ldapUserRDN
The adapter maps the value of the LDAP **CN** attribute to the **ERUID** and **CN** attributes of the Identity server. The number of values for the LDAP **CN** attributes affects the mapping.

pwdChangeTime attribute for the LDAP Adapter
When a password policy is enabled, the **pwdChangedTime** attribute is set on the resource for each person or user entry when the password is changed by an administrator.

Commas in the cn attribute
If you use commas in the **cn** attribute, the following guidelines apply:

Support for the pwdReset attribute
When password policy is enabled, the **pwdReset** attribute is set on the resource for each person or user entry when the password is changed by an administrator.

RDN attribute change for the group account
To change the RDN attribute for a group account, change these files to map the **cn** attribute to the required RDN attribute:

Base point configuration
The base point for the LDAP Adapter is the point in the directory server that is used as the root for the adapter. The base point can be an organizational unit (OU) or domain container (DC) base point.

Related tasks

Adding support for a new user/group object class

You can add support for a new user/group object class.

Adding support for a new directory server
You can add support for a new directory server.

Enabling SSL communication

Use this procedure to configure secure communications between the LDAP server and Security Directory Integrator.

About this task

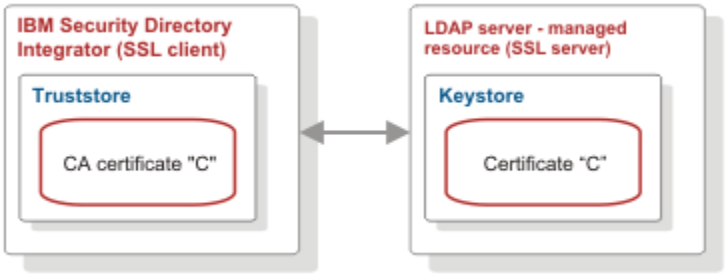

Figure 4. One-way SSL authentication (managed LDAP server authentication)

To configure one-way SSL, perform the following tasks. For instructions about the individual tasks, see the SSL information in the *IBM Security Dispatcher Installation and Configuration Guide*.

Procedure

1. Create a keystore for the Security Directory Integrator server.
2. Create a truststore for the Security Directory Integrator server.
3. Configure Security Directory Integrator to use the keystores.

   Note: The editing of the solution.properties file for steps 6, 7, and 8 can be done in one operation. Doing so eliminates the need for a stop and restart of the adapter service at the end of steps 6 and 7.
4. Configure Security Directory Integrator to use the truststores.
5. Enable the adapter service to use SSL.
6. Create a certificate and CA certificate for the managed LDAP server. For more information about configuring SSL on the LDAP server, See the following resources on the web:

   IBM Tivoli Directory Server
   http://www-01.ibm.com/support/knowledgecenter/SSVJJU_6.3.0/com.ibm.IBMDS.doc/welcome.html

   Sun ONE Directory Server
   http://docs.sun.com/source/816-6698-10/ssl.html#14416
7. Import the CA certificate for the managed LDAP server into the Security Directory Integrator truststore.

   This step is similar to importing the Identity server CA certificate in the WebSphere® Application Server truststore. Use the CA certificate for the LDAP server instead of the CA certificate for WebSphere.
8. Stop and restart the adapter service.

   See Start, stop, and restart the adapter service.

Verifying that the adapter is working correctly

After you install and configure the adapter, verify that the installation and configuration are correct.

Procedure

1. Test the connection for the service that you created on the Identity server.
2. Run a full reconciliation from the Identity server.
3. Run all supported operations such as add, modify, and delete on one user account.
4. Verify the `ibmdi.log` file after each operation to ensure that no errors are reported.
5. Verify the `trace.log` file to ensure that no errors are reported when you run an adapter operation.

Related concepts

Installing the dispatcher
If this is the first Security Directory Integrator-based adapter installation, you must install the RMI Dispatcher before you install the adapter. Install the RMI Dispatcher on the same Security Directory Integrator server where you want to install the adapter.

Restarting the adapter service
Various installation and configuration tasks might require the adapter to be restarted to apply the changes. For example, you must restart the adapter if there are changes in the adapter profile, connector, or assembly lines. To restart the adapter, restart the Dispatcher.

Service/Target form details
Complete the service/target form fields.

Installing the adapter language package
The adapters use a separate language package from IBM Security Verify Identity.

Related tasks

Installing the adapter binaries or connector
The connector might or might not be available with the base Security Directory Integrator or Security Directory Integrator product. The connector is required to establish communication between the adapter and the Dispatcher.

Importing the adapter profile
An adapter profile defines the types of resources that the Identity server can manage. It is packaged with the IBM Security Verify Adapter. Use the adapter profile to create an adapter service on Identity server and establish communication with the adapter.

Creating an adapter service/target
After you import the adapter profile on the Identity server, create a service/target so that Identity server can communicate with the managed resource.

Chapter 6. Troubleshooting

Troubleshooting is a systematic approach to solving a problem. The goal of troubleshooting is to determine why something does not work as expected and how to resolve the problem. This topic provides information and techniques for identifying and resolving problems that are related to the adapter, including troubleshooting errors that might occur during the adapter installation.

Techniques for troubleshooting problems

Certain common techniques can help with the task of troubleshooting. The first step in the troubleshooting process is to describe the problem completely.

Problem descriptions help you and the IBM technical-support representative find the cause of the problem. This step includes asking yourself basic questions:

- What are the symptoms of the problem?
- Where does the problem occur?
- When does the problem occur?
- Under which conditions does the problem occur?
- Can the problem be reproduced?

The answers to these questions typically lead to a good description of the problem, which can then lead you to a problem resolution.

What are the symptoms of the problem?

When you start to describe a problem, the most obvious question is "What is the problem?" This question might seem straightforward; however, you can break it down into several more-focused questions that create a more descriptive picture of the problem. These questions can include:

- Who, or what, is reporting the problem?
- What are the error codes and messages?
- How does the system fail? For example, is it a loop, hang, crash, performance degradation, or incorrect result?

Where does the problem occur?

Determining where the problem originates is not always easy, but it is one of the most important steps in resolving a problem. Many layers of technology can exist between the reporting and failing components. Networks, disks, and drivers are only a few of the components to consider when you are investigating problems.

The following questions help you to focus on where the problem occurs to isolate the problem layer:

- Is the problem specific to one operating system, or is it common across multiple operating systems?
- Is the current environment and configuration supported?
- Do all users have the problem?
- (For multi-site installations.) Do all sites have the problem?

If one layer reports the problem, the problem does not necessarily originate in that layer. Part of identifying where a problem originates is understanding the environment in which it exists. Take some time to completely describe the problem environment, including the operating system and version, all corresponding software and versions, and hardware information. Confirm that you are running within an environment that is a supported configuration. Many problems can be traced back to incompatible levels of software that are not intended to run together or are not fully tested together.

When does the problem occur?

Develop a detailed timeline of events that lead up to a failure, especially for those cases that are one-time occurrences. You can most easily develop a timeline by working backward: Start at the time an error was reported (as precisely as possible, even down to the millisecond), and work backward through the available logs and information. Typically, you use the first suspicious event that you find in a diagnostic log.

To develop a detailed timeline of events, answer these questions:

- Does the problem happen only at a certain time of day or night?
- How often does the problem happen?
- What sequence of events leads up to the time that the problem is reported?
- Does the problem happen after an environment change, such as upgrading or installing software or hardware?

Responding to these types of questions can give you a frame of reference in which to investigate the problem.

Under which conditions does the problem occur?

Knowing which systems and applications are running at the time that a problem occurs is an important part of troubleshooting. These questions about your environment can help you to identify the root cause of the problem:

- Does the problem always occur when the same task is being done?
- Is a certain sequence of events required for the problem to occur?
- Do any other applications fail at the same time?

Answering these types of questions can help you explain the environment in which the problem occurs and correlate any dependencies. Remember that just because multiple problems might occur around the same time, the problems are not necessarily related.

Can the problem be reproduced?

From a troubleshooting standpoint, the ideal problem is one that can be reproduced. Typically, when a problem can be reproduced you have a larger set of tools or procedures at your disposal to help you investigate. Problems that you can reproduce are often easier to debug and solve.

However, problems that you can reproduce can have a disadvantage: If the problem is of significant business impact, you do not want it to recur. If possible, re-create the problem in a test or development environment, which typically offers you more flexibility and control during your investigation.

- Can the problem be re-created on a test system?
- Do multiple users or applications have the same type of problem?
- Can the problem be re-created by running a single command, a set of commands, or a particular application?

Error messages and problem solving

A warning or error message might be displayed in the user interface to provide information about the adapter or when an error occurs.

Table 5 on page 45 contains warnings or errors which might be displayed in the user interface if the LDAP Adapter is installed on your system.

Table 5. Warning and error messages

Warning or error message	Recommended Action
No login or an invalid credential was supplied in the request.	The adapter cannot bind to a naming context or is unable to initialize because invalid credentials were provided. To fix this problem, ensure that: • The managed resource is functioning properly and that you are connected to the correct resource. • The naming context is correct if the naming context is customized. • The administrator ID specified on the service form is correct. • The administrator password specified on the service form is correct.
An error occurred while establishing communication with the Security Directory Integrator server.	Identity server cannot establish a connection with Security Directory Integrator. To fix this problem, ensure that: • Security Directory Integrator is running • The URL specified on the service form for Security Directory Integrator is correct.
Insufficient 'add' privilege.	The administrator ID that is specified on the service form does not have privileges to add a user under the base DN. You must change the administrator ID to an administrator ID that has the correct privileges or assign privileges for the specified administrator ID.
Entry Already Exists or exception:javax.naming.NameAlreadyBoundException.	The user has already been added to the resource. This error might occur if you are attempting to add a user to the directory server and Identity server is not synchronized with the resource. To fix this problem, schedule a reconciliation between Identity server and the resource. See the online help for information about scheduling a reconciliation.
Unknown Error while adding entry on resource.	This error might occur for several reasons. To fix this problem, ensure that: • The administrator ID specified on the service form is correct. • The administrator password specified on the service form is correct. • The base point is correct, if it is customized. • The administrator ID has the correct privileges to modify a user account under the base DN. • The network connection is not slow.
Cannot add user to specific group.	If you cannot add a user to a group, ensure that the specified group was created on the resource.

Table 5. Warning and error messages (continued)

Warning or error message	Recommended Action
User not found.	This error might occur when you attempt to add, modify, delete, or search for a user. This error might also occur if you attempt to change the password for a user. To fix the problem, ensure that: • The server that is specified for the adapter is correct. • The administrator ID specified on the service form is correct. • The administrator password specified on the service form is correct. • The base point is correct, if it is customized. If the error continues to occur, check to ensure that • The user was created on the directory server. • The user was not moved or deleted from the directory server. To fix the problem, add the user to the directory server and then schedule a reconciliation. See the online help for information about scheduling a reconciliation.
Unknown error while modifying entry on resource.	This error might occur for several reasons. To fix this problem, ensure that: • The administrator ID specified on the service form is correct. • The administrator password specified on the service form is correct. • The base point is correct, if it is customized. • The administrator ID has the correct privileges to modify a user account under the base DN. • The network connection is not slow.
Error adding user to group.	If you cannot add a user to a group, ensure that • The user was created on the resource. • The user is not already a member of the group. • The group was created on the resource. If the user does not exist on the resource, you must create the user. If a user is already a member of a group, you cannot add the user to the group. If the group does not exist on the resource, you must add the group to the resource before you can add a user to the group. See the online help for information about creating groups or adding users to groups.
Insufficient 'delete' privilege.	The administrator ID that is specified on the service form does not have privileges to delete a user under the base DN. You must change the administrator ID to an administrator ID that has the correct privileges or assign privileges for the specified administrator ID.

Table 5. Warning and error messages (continued)	
Warning or error message	**Recommended Action**
Search failed.	This error might occur for several reasons. To fix the problem, ensure that: • The network connection is not slow. • The resource is not overloaded with network traffic. • Security Directory Integrator has sufficient memory, if you have a large number of users and groups.
Reconciliation operation stops prematurely with Out of Memory error.	1. Open the service.def file from the LdapProfile.jar archive. 2. Locate the line containing name="ldapPageSize" and change the default value from 0 to 100. 3. If you are using a Directory Server other than IBM Security Directory Server, also change "ldapPageSize" to "ldapVLVPageSize". For more information on modifying LdapProfile.jar, see “Customizing the adapter profile” on page 25.
Group already exists.	The group name that you specified already exist on the managed resource. Create a group with another group name.
Specified attribute violates the schema.	This error occurs when the following attributes are not in the DN format: • Group Owner • See Also Ensure that the values of Group Owner and See Also attributes are in the DN format. For example, you can add a user in the following format for the Group Owner and See Also attributes:`cn=`*`user1`*`,dc=`*`com`*.
Group not found.	Perform a reconciliation operation to ensure that the group exists on the managed resource.
Schema violation.	This error occurs when the Group RDN attribute is other than CN and the value of CN is blank for the Group Full Name attribute on the group form. Ensure that you select the CN option for the **Group RDN attribute** on the service form or specify a value for the Group Full Name attribute on the group form.

Handling memory problems in the adapter

During reconciliation requests, some directory servers return the entire search result in one chunk or page (for example, none paged search), which typically causes memory problems.

About this task

It might appear that the LDAP Adapter has a memory leak, but the adapter is processing the entries from the directory server while the server continues to add more entries.

If you are managing an IBM Security Directory Server as your LDAP server, this is not an issue because the IBM Security Directory Server supports paging.

Note: If you are managing an LDAP directory server other than IBM Security Directory Server, see the vender's directory server help for information regarding paged search. Additional IBM Security Directory Server information regarding memory problems are available on the Web in the *IBM Security Directory Integrator Reference Guide*.

Follow these steps to enable paged search:

Procedure

1. Open the `service.def` file from the `LdapProfile.jar` archive.
2. Locate the line containing name="ldapPageSize" and change the default value from `0` to `100`.

   For more information on modifying `LdapProfile.jar`, see “Customizing the adapter profile” on page 25.

Chapter 7. Uninstalling

To remove an adapter from the Identity server for any reason, you must remove all the components that were added during installation. Uninstalling the adapter involves running the uninstaller and removing the adapter profile from the Identity server.

Deleting the adapter profile

Remove the adapter service/target type from the Identity server. Before you delete the adapter profile, ensure that no objects exist on the Identity server that reference the adapter profile.

Objects on the Identity server that can reference the adapter profile:

- Adapter service instances
- Policies referencing an adapter instance or the profile
- Accounts

Note: The Dispatcher component must be installed on your system for adapters to function correctly in a Security Directory Integrator environment. When you delete the adapter profile, do not uninstall the Dispatcher.

For specific information about how to delete the adapter profile, see the IBM Security Verify Identity product documentation.

Index

T

U

V

W