IBM Security Verify Governance Identity Manager

CLIx Adapter Installation and Configuration Guide

Contents

Figures

Tables

Chapter 1. Overview

An adapter is an interface between a managed resource and the Identity server.

Adapters might be installed on the managed resource. The Identity server manages access to the resource by using your security system. Adapters function as trusted virtual administrators on the target platform. They perform tasks, such as creating, suspending, and restoring user accounts, and other administrative functions that are performed manually. The adapter runs as a service, independently of whether you are logged on to the Identity server.

The CLIx Adapter enables communication between the Identity server and a resource that provides a command-line interface.

Architecture

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

- The Dispatcher
- The Security Directory Integrator connector
- IBM Security Verify Adapter profile

You need to install the 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 1 describes the components that work together to complete the user account management tasks in a Security Directory Integrator environment.

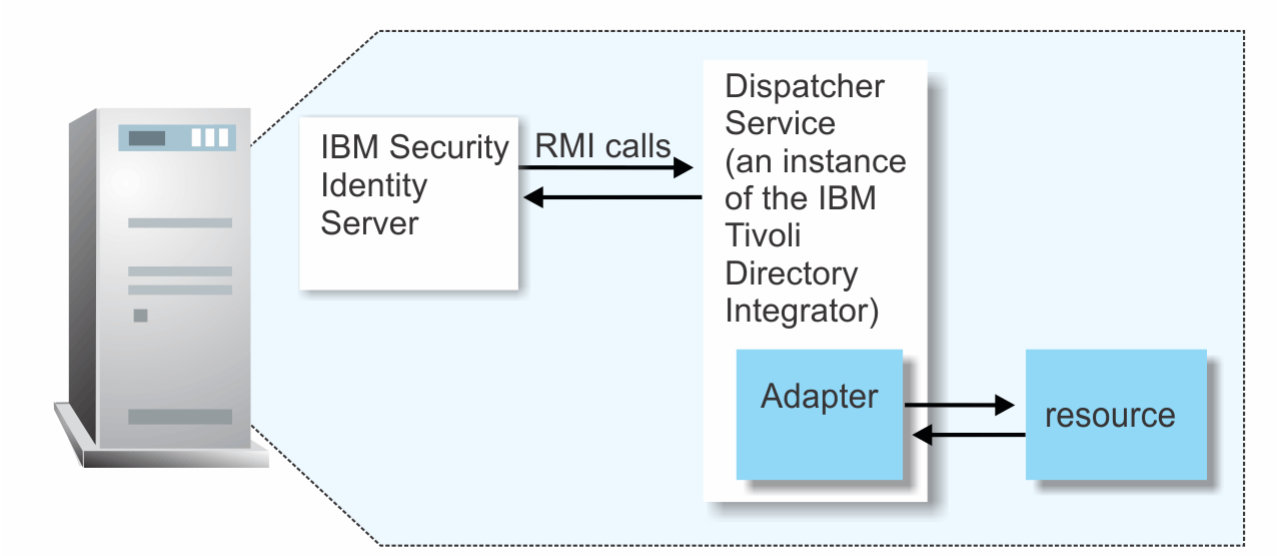

Figure 1. The architecture of the CLIx Adapter

Supported configurations

The adapter supports both single and multiple server configurations.

- The Identity server
- The Tivoli® Directory Integrator server
- The managed resource
- The Security Directory Integrator CLIx 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 CLIx Adapter on one server to establish communication with the managed resource. The managed resource is installed on a different server as described in Figure 2 on page 2.

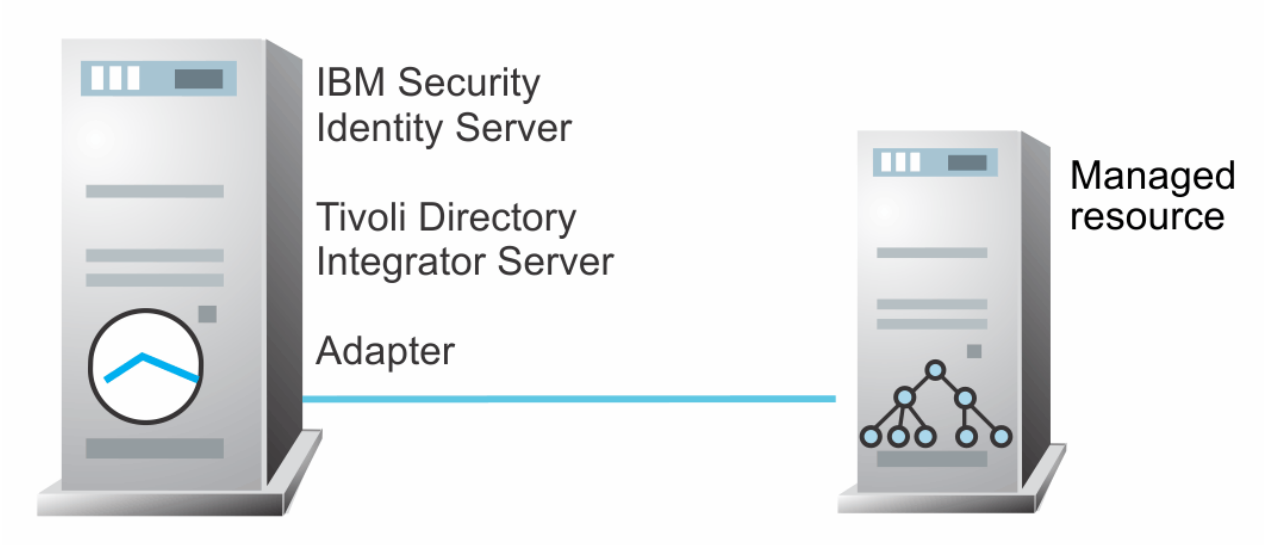

Figure 2. Example of a single server configuration

Multiple server configuration

In a multiple server configuration, the Identity server, the Security Directory Integrator server, the CLIx Adapter, and the managed resource are installed on different servers. Install the Security Directory Integrator server and the CLIx Adapter on the same server as described in Figure 3 on page 2.

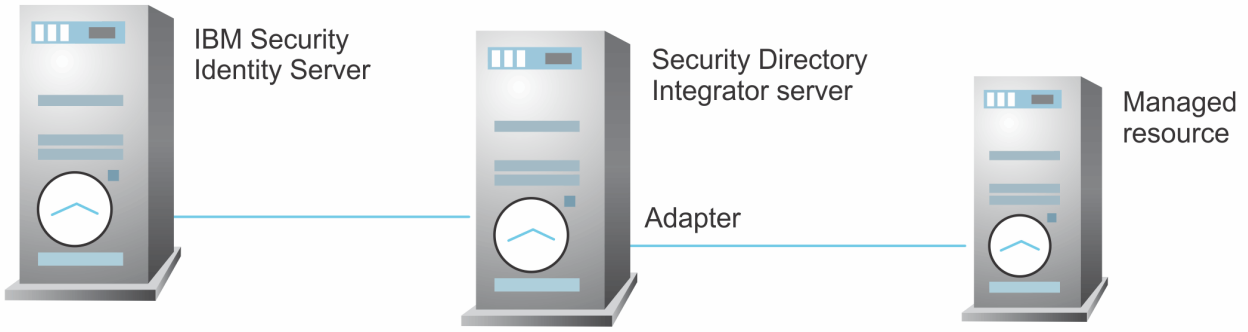

Figure 3. Example of multiple server configuration

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 Governance Identity Manager

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

Note: There is a separate instruction for installing, upgrading or uninstalling adapters from the IBM Security Verify Governance Identity Manager virtual appliance.

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. Load attribute mapping.
8. Set account defaults.
9. Create an adapter service/target.
10. Install the adapter language package.
11. 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.

The following table 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. Prerequisites to install 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
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. For more information, see the *Dispatcher Installation and Configuration Guide*.

Note: Set the environmental variable CLASSPATH to Java version 1.5 that is required for the adapter installation or upgrade.

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

Related concepts

Roadmap for IBM Security Directory Integrator based adapters, for IBM Security Verify Governance Identity Manager
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 Governance Identity Manager 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 Governance Identity Manager
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. 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 adapter jars. For example, the jars/connectors subdirectory contains the jar for the UNIX adapter.	If Security Directory Integrator is automatically installed with the Identity server, the default directory path for Security Directory Integrator is as follows:
		Windows:
		• for version 7.2:
		`drive\Program Files \IBM\TDI\V7.2`
		UNIX:
		• for version 7.0:
		`/opt/IBM/TDI/V7.2`

Table 2. Required information to install the adapter (continued)		
Required information	**Description**	**Value**
Adapters solution 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*.	The default solution directory is located at: **Windows:** • for version 7.2: *drive*\Program Files \IBM\TDI\V7.2*timsol* **UNIX:** • for version 7.2: /opt/IBM/TDI/V7.2/ *timsol*

Related concepts

Roadmap for IBM Security Directory Integrator based adapters, for IBM Security Verify Governance Identity Manager

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 Verify the adapter installation.

The Security Directory Integrator CLIx Adapter uses the Security Directory Integrator CLIx connector. This connector is not available with the base Security Directory Integrator product. The Security Directory Integrator CLIx Adapter installation consists of installing the Security Directory Integrator CLIx connector and importing the Security Directory Integrator CLIx Adapter profile.

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*.

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.

Procedure

1. Create a temporary directory on the workstation where you want to install the adapter.
2. Extract the contents of the compressed file in the temporary directory.
3. Copy the `CLConnector.jar` file from the adapter package to the *`ITDI_HOME`*`/jars/connectors` directory.
4. Copy the command-line script files to the `ADAPTER_SOLDIR` directory.

   The CLIx adapter package provides a complete set of sample command-line batch files.
5. Restart the adapter service.

Verifying the adapter installation

If the adapter is installed correctly, the required components exist in the specified directory.

Table 3. Adapter component

Adapter component	Directory
`CLConnector.jar`	**On the Windows operating system** *drive*`:\Program Files\IBM\TDI\7.2\jars\connectors\` **On the UNIX operating system** `/opt/IBM/TDI/V7.2/jars/connectors/`

Review the installer log file `CLIXAdapter_Installer.log` that is in the adapter installer directory for any errors.

If this installation is to upgrade a connector, then send a request from IBM Security Verify Identity. Verify that the version number in the `ibmdi.log` matches the version of the connector that you installed. The `ibmdi.log` file is in the *ITDI_Home*`\`*adapter solution directory*`\logs` directory.

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*.

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

- The Identity server is installed and running.
- 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 the IBM Security Identity Governance and Intelligence is located in the `IGI-profile` folder of the installation package.

About this task

Target 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. On the Appliance Dashboard, select Verify Governance Identity Manager Administration Console from the **Quick Links** widget.

   The Administration Console is displayed.
2. From the Administration Console, select **Target Administration**.

   The Target Administration console is displayed.
3. From the navigation tree, select **Manage Target Types**.

   The **Manage Target Types** page is displayed.
4. On the **Manage Target Types** page, click **Import**.

   The **Import Target Type** page is displayed.
5. On the **Import Target Type** page, complete these steps:
   a) In the **Target Definition File** field, click **Browse** to locate the <*Adapter*>`Profile.jar` 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**.

      A message indicates that you successfully imported a target type.
6. Click **Close**.

What to do next

- The import occurs asynchronously, which means it might take some time for the target type to load into the Identity server from the properties files and to be available in other pages. On the **Manage Target Types** page, click **Refresh** to see the new target type. If the target type is not displayed in a reasonable amount of time, 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. On the Appliance Dashboard, select **Manage System Settings** > **Maintenance** > **Log Retrieval and Configuration** > **Identity** > **trace log**, then click **View**.

Attribute Mapping

Attribute mapping is required to define which target attributes correspond to the Verify Governance Identity Manager account attributes.

About this task

This task involves an account attribute mapping definition file, which is included in the adapter package.

The file consists of Verify Governance Identity Manager account attributes and their equivalent attributes in the managed target. The file is structured as *<IGI_attribute> = <target_attribute>*.

The *<IGI_attribute>* is fixed and must not be modified. Edit only the *<target_attribute>*. Some *<IGI_attribute>* already has a fixed equivalent *<target_attribute>* of `eraccount`.

Some *<IGI_attribute>* do not have a defined *<target_attribute>* and you can assign the mapping. For example:

```
USER_TYPE=USER_TYPE
ATTR1=ATTR1
```

Note:

- The default mapping is already included out-of-the box. If there are no changes to the attribute mapping, there is no need to import the attribute mapping files.
- It might take up to 10 minutes for the attribute mapping changes to take effect once the file is imported.

Procedure

1. Open the mapping definition file by using any text editor.
2. Edit the mapping.
3. If the target attribute has a list of predefined values, use the following syntax to convert its values to the corresponding Verify Governance Identity Manager attribute values.

```
[conversion].<target_attribute>.<IGI_attribute> =
[<target_attribute_value1>=<IGI_attribute_value1>;...;
<target_attribute_valuen>=<IGI_attribute_valuen>]
```

4. For attributes that contains date and time, use the following syntax to convert its values.
   For example:

```
[conversion.date].erbirthDate.BIRTHDAY=[yyyyMMdd=dd/MM/yyyy HH:mm:ss]
[conversion.date].ACCOUNT_EXPIRY_DATE.ACCOUNT_EXPIRY_DATE=
[dd/MM/yyyy HH:mm:ss=dd/MM/yyyy HH:mm:ss]
```

5. Import the updated mapping definition file through the Enterprise Connectors module. For more information, see *Attribute-to-permission mapping service* in the IBM Security Verify Governance Identity Manager product documentation.
6. Map the following attributes for **Chanel-Write To** and **Chanel-Read From**

Attribute	Mapped Attribute
eruid	CODE
erpassword	PASSWORD

   For more information, see *Mapping attributes for a connector* in the IBM Security Verify Governance Identity Manager product documentation.

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 10.

About this task

You must create an administrative user account for the adapter on the managed resource. Provide the account information when you create a target. 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.

Use the target form to provide information for the target. The actual target form fields might vary depending on whether the service form is customized. The target name and description that you provide for each target are displayed on the console. Therefore, it is important to provide values that make sense to your users and administrators.

Procedure

1. On the Appliance Dashboard, select Verify Governance Identity ManagerAdministration Console from the **Quick Links** widget.

   The Administration Console is displayed.
2. From the Administration Console, select **Target Administration**.

   The Target Administration console is displayed.

3. From the navigation tree, click **Manage Targets**.

   The **Select a Target** page is displayed.
4. On the **Select a Target** page, click **Create**.

   The **Create a Target** wizard is displayed.
5. On the **Select the Type of Target** page, select a target type and 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 **General Information** page, specify the values for the target instance.

   The content of the **General Information** page depends on the type of target that you are creating. The creation of some targets might require more steps. It is specific to the profile (adapter). See the adapter's *Installation and Configuration Guide* for the more information.
7. On the **Users and Groups** page, which is displayed only for LDAP targets, complete the required fields.
8. On the **Authentication** page, which does not display for every target type, complete the required fields.
9. On the **Dispatcher Attributes** page, specify information about the dispatcher attributes and click **Next** or **OK**.

   The **Dispatcher Attributes** page is displayed only for IBM Security Directory Integrator based targets.
10. On the **Status and Information** page, view information about the adapter and managed resource and click **Next** or **Finish**.

    The adapter must be running to obtain the information.
11. On the **Application Information** page, type a name and description for the application, and then click **Finish**.
12. Optional: 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 target instance for a specific target type.

Service/Target form details

Complete the service/target form fields.

On the General Information 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`.

The following table shows the ports that are open in the firewall for every instance that is created. However, usage of these port numbers do not support high availability.

Table 4. Ports

Instance	Ports
SDI1	1199, 1198, 1197, 1196, 1195, 1194
SDI2	2299, 2298, 2297, 2296, 2295, 2294
SDI3	3399, 3398, 3397, 3396, 3395, 3394
SDI4	4499, 4498, 4497, 4496, 4495, 4494
SDI5	5599, 5598, 5597, 5596, 5595, 5594
SDI6	6699, 6698, 6697, 6696, 6695, 6694
SDI7	7799, 7798, 7797, 7796, 7795, 7794
SDI8	8899, 8898, 8897, 8896, 8895, 8894
SDI9	9999, 9998, 9997, 9996, 9995, 9994
SDI10	11099, 11098, 11097, 11096, 11095, 11094

For a high availability implementation, use any of these port numbers.

- 1099
- 2099
- 3099

Administrator Name
Specify the administrator user that is used to log in to the resource and perform user management operations on the managed resource. This name is the same account that you created on the managed resource for the adapter. See Adapter user account creation.

Administrator Password
Specify the password for administrator user.

Add request command
Specify the command that adds users to the resource.

Modify request command
Specify the command that modifies users on the resource.

Delete request command
Specify the command that deletes users from the resource.

Search request command
Specify the command that reconciles users from the resource.

Test request command
Specify the command that tests the connection to the resource.

Search supporting data request command
Specify the command that reconciles supporting data from the resource.

Owner
Optional: Specify a user as a service owner.

Service Prerequisite
Optional: Specify a service that is prerequisite to this service.

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, and delete 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: `c:\Program Files\IBM\TDI\V7.2\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/V7.2/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 10 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.

Server Host Name
Specify the managed resource on which you want to control the maximum connections by using the dispatcher property Max Connection Count.

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 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.

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.

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 9.

Upgrading the adapter binaries or connector

Before you upgrade the connector, stop the dispatcher service.

You can upgrade the connector by copying the new connector JAR file to the appropriate installation directory, which is typically the *ITDI_HOME*/jars/connectors directory.

Upgrading the adapter profile

Read the adapter Release Notes® for any specific instructions before you import a new 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.

You can use several options when you configure the CLIx Adapter.

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

Editing the IBM Security Verify Identity CLIx 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.

Related concepts

Maximum length of the account form attributes
When you want to modify the maximum length of the attributes on the account form, modify the `schema.dsml` file with their required length.

Password management for account restoration
When an account is restored from being previously suspended, you are prompted to supply a new password for the reinstated account.

Related tasks

Creating a JAR file and importing the profile on the IBM Security Verify Identity

After you modify the `schema.dsml` or any other profile files, you must import the profiles into IBM Security Verify Identity for the changes to take effect.

Maximum length of the account form attributes

When you want to modify the maximum length of the attributes on the account form, modify the `schema.dsml` file with their required length.

For example, when you want the First Name attribute's maximum length to 2048, modify the `schema.dsml` file as:

```
Old profile:

<!-- ******************************************************** -->
<!-- erRsaAmFirstName -->
<!-- ******************************************************** -->
<attribute-type single-value = "true" >
    <name>erRsaAmFirstName</name>
    <description>First Name</description>
    <object-identifier>1.3.6.1.4.1.6054.3.150.2.1</object-identifier>
    <syntax>1.3.6.1.4.1.1466.115.121.1.15{1024}</syntax>
</attribute-type>

Modified profile:

<!-- ******************************************************** -->
<!-- erRsaAmFirstName -->
<!-- ******************************************************** -->
<attribute-type single-value = "true" >
    <name>erRsaAmFirstName</name>
    <description>First Name</description>
    <object-identifier>1.3.6.1.4.1.6054.3.150.2.1</object-identifier>
    <syntax>1.3.6.1.4.1.1466.115.121.1.15{2048}</syntax>
</attribute-type>
```

Related concepts

Password management for account restoration
When an account is restored from being previously suspended, you are prompted to supply a new password for the reinstated account.

Related tasks

Editing the IBM Security Verify Identity CLIx 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.

Creating a JAR file and importing the profile on the IBM Security Verify Identity
After you modify the `schema.dsml` or any other profile files, you must import the profiles into IBM Security Verify Identity for the changes to take effect.

Creating a JAR file and importing the profile on the IBM Security Verify Identity

After you modify the `schema.dsml` or any other profile files, you must import the profiles into IBM Security Verify Identity for the changes to take effect.

About this task

In order to install the new attributes, complete the following steps:

Note: If you are upgrading an existing adapter profile, the new adapter profile schema is not reflected immediately. You need to stop and start the IBM Security Verify Identity server to refresh the cache and the adapter schema. For more information about upgrading an existing adapter, see Chapter 4, “Upgrading,” on page 17.

Procedure

1. Extract the contents of the `TDICLIXProfile.jar` file into the temporary directory by running the following command:

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

   The **`jar`** command creates the *c*`:\temp\TDICLIXProfile` directory.
2. Update the profile files.
3. Create a JAR file with the files in the `\temp` directory by running the following commands:

   ```
   cd c:\temp
   jar -cvf TDICLIXProfile.jar TDICLIXProfile
   ```

4. Import the `TDICLIXProfile.jar` file into the IBM Security Verify Identity server.

   For more information about importing the file, see Importing the adapter profile.
5. Stop and start the IBM Security Verify Identity server.

Related concepts

Maximum length of the account form attributes
When you want to modify the maximum length of the attributes on the account form, modify the `schema.dsml` file with their required length.

Password management for account restoration
When an account is restored from being previously suspended, you are prompted to supply a new password for the reinstated account.

Related tasks

Editing the IBM Security Verify Identity CLIx 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.

Password management for account restoration

When an account is restored from being previously suspended, you are prompted to supply a new password for the reinstated account.

However, in some cases you might not want to supply a new password.

How each restore action interacts with its corresponding managed resource depends on either the managed resource, or the business processes that you implement. Certain resources reject a password when a request is made to restore an account. In this case, you can configure IBM Security Verify Governance Identity Manager to forego the new password requirement. You can set the CLIx Adapter to require a new password when the account is restored, if your company has a business process in place that dictates that the account restoration process must be accompanied by resetting the password.

In the service.def file, you can define whether a password is required as a new protocol option. When you import the adapter profile, if an option is not specified, the adapter profile importer determines the correct restoration password behavior from the schema.dsml. Adapter profile components also enable remote services to find out whether you discard a password that is entered by the user in a situation where multiple accounts on disparate resources are being restored. In this situation, only some of the accounts being restored might require a password. Remote services discard the password from the restore action for those managed resources that do not require them.

Edit the service.def file to add the new protocol options, for example:

```
<Property Name  = "com.ibm.itim.remoteservices.ResourceProperties.
                  PASSWORD_NOT_REQUIRED_ON_RESTORE"><value>true</value>
</property>
<Property Name  = "com.ibm.itim.remoteservices.ResourceProperties.
                  PASSWORD_NOT_ALLOWED_ON_RESTORE"><value>false</value>
</property>
```

By adding the two options in the preceding example, you are ensuring that you are not prompted for a password when an account is restored.

Related concepts

Maximum length of the account form attributes
When you want to modify the maximum length of the attributes on the account form, modify the `schema.dsml` file with their required length.

Related tasks

Editing the IBM Security Verify Identity CLIx 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.

Creating a JAR file and importing the profile on the IBM Security Verify Identity
After you modify the `schema.dsml` or any other profile files, you must import the profiles into IBM Security Verify Identity for the changes to take effect.

Chapter 6. Uninstalling

To remove an adapter from the Identity server for any reason, you must remove all the components that were added during installation. Uninstalling an IBM Security Directory Integrator based adapter mainly involves removing the connector file, and the adapter profile from the Identity server. Depending on the adapter, some of these tasks might not be applicable, or there can be other tasks.

Removing the adapter binaries or connector

The CLIx Adapter installation process also installs the Security Directory Integrator CLIx connector. You must uninstall the adapter from the Security Directory Integrator server to completely uninstall the CLIx adapter.

Procedure

1. Stop the adapter service.
2. Remove the `CLIxConnector.jar` file from the *`ITDI_HOME`*`/jars/connectors` directory.
3. Start the service.

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 Governance Identity Manager product documentation.

Index