IBM Security Verify Identity
7.0

Documentum Content Server 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 reside 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 TDI-based Documentum Server Adapter enables communication between the Identity server and the Documentum Content Server.

Features of the adapter

The adapter automates several administrative and management tasks.

- Adding user accounts
- Modifying user account attributes
- Modifying user account passwords
- Suspending, restoring, and deleting user accounts
- Reconciling user accounts and 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.

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

You always must 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 2 describes the components that work together to complete the user account management tasks in a Security Directory Integrator environment.

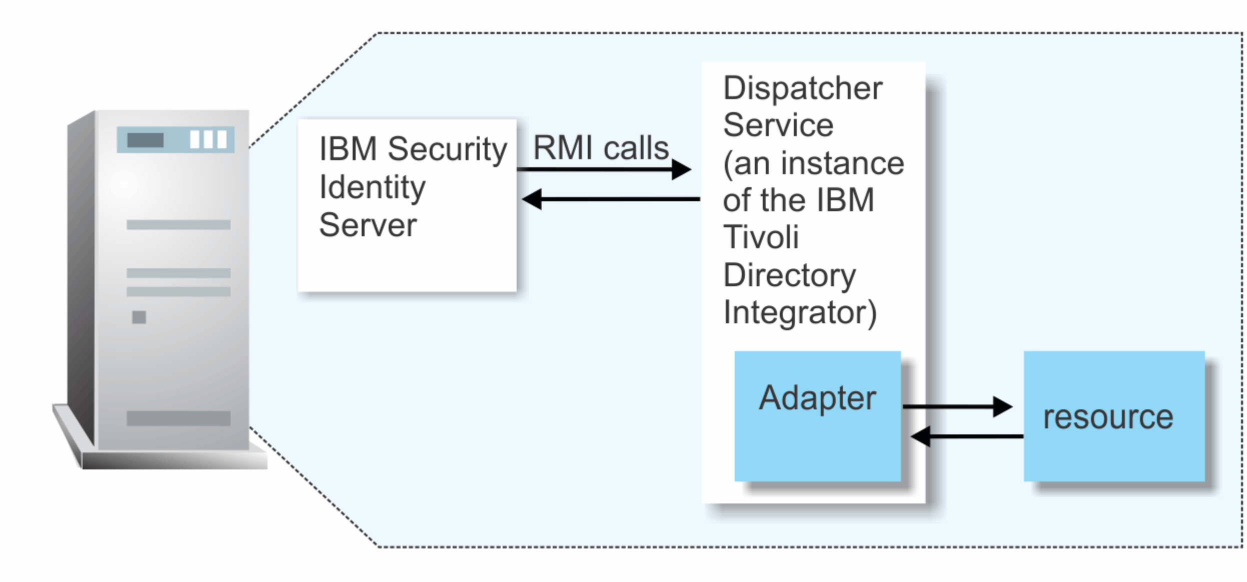
IBM Security Identity Server
RMI calls
Dispatcher Service (an instance of the IBM Tivoli Directory Integrator)
Adapter
resource

Figure 1. The architecture of the TDI-based Documentum Server Adapter

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 Security Directory Integrator server
- The managed resource
- The adapter

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

Single server configuration

Install the Identity server, the Security Directory Integrator server, and the TDI-based Documentum Server Adapter on one server.

This configuration establishes communication with the Documentum Content Server. The Documentum Content Server is installed on a different server as described in Figure 2 on page 3.

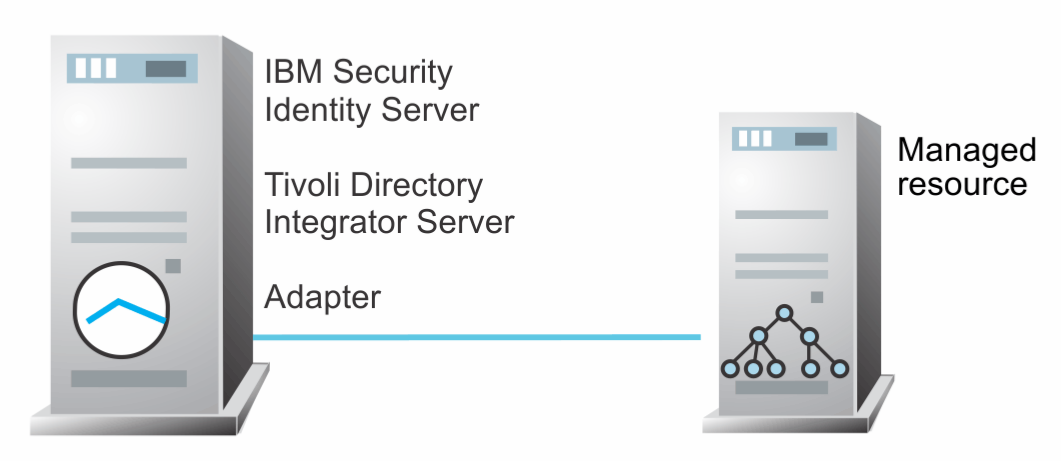

Figure 2. Example of a single server configuration

Multiple server configuration

Install the Identity server, the Security Directory Integrator server, the TDI-based Documentum Server Adapter, and the Documentum Content Server on different servers.

Install the Security Directory Integrator server and the TDI-based Documentum Server Adapter on the same server as described in Figure 3 on page 3.

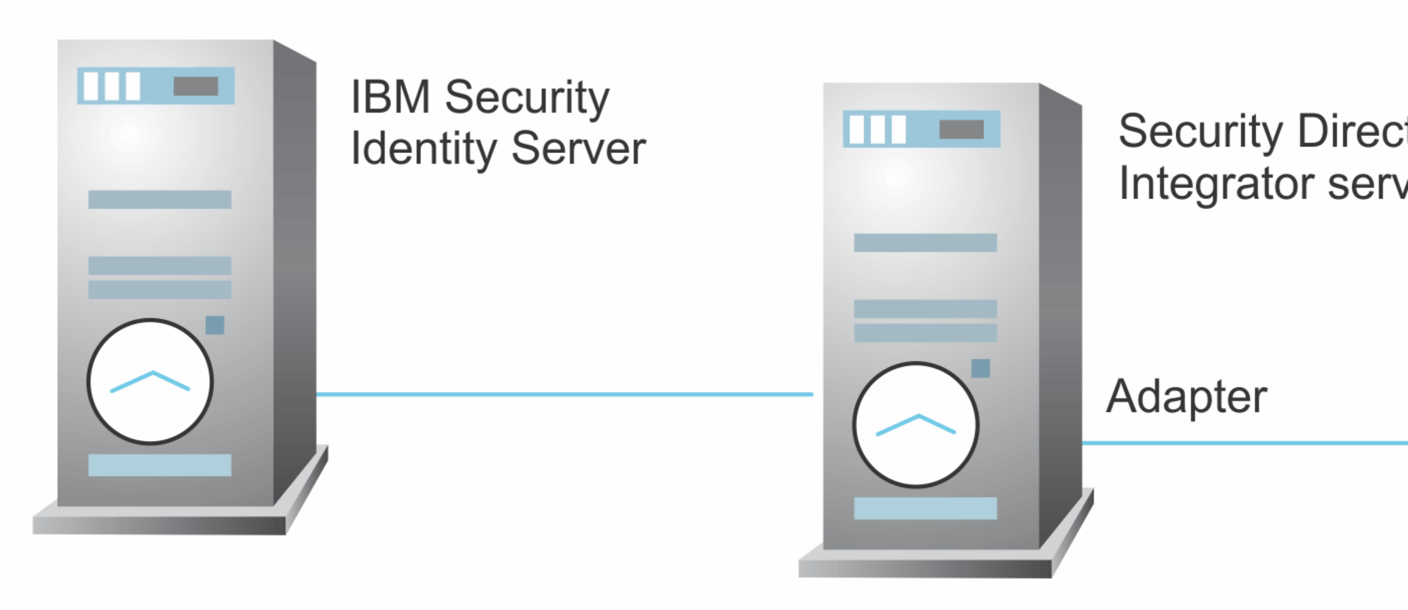

Figure 3. Example of multiple server configuration

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

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 IBM 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
Documentum Content Server	Documentum Content Server 7.0 Documentum Content Server 7.1
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*.

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

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.

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 directories to install the adapter

Required information	**Description**
Security Directory Integrator Home Directory	The *ITDI_HOME* directory contains the `jars/connectors` subdirectory that contains adapter jar files.
Adapters solution directory	When you install the dispatcher, the installer prompts you to specify a file path for the solution directory. See the *Dispatcher Installation and Configuration Guide*.

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.

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

Verifying the adapter installation
If the adapter is installed correctly, required components exist in the specified directories.

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.

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

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

See the Release Notes bundled with this adapter package for updates on installation and configuration steps.

About this task

The adapter uses the Documentum Content Server connector. The connector is not available with the base Security Directory Integrator product. The adapter installation involves the TDI-based Documentum Server Adapter connector installation. Before you install the adapter, make sure that the RMI Dispatcher is already installed.

Procedure

1. Create a temporary directory on the workstation where you want to extract the adapter.
2. Extract the contents of the compressed file in the temporary directory.
3. Copy the `connectors/DocumentumConnector.jar` file to the `*ITDI_HOME*/jars/connectors` directory.
4. Restart the adapter service.
5. Copy the DFC API JAR files. See "Copying DFC API JAR files from the Documentum Content Server to the Security Directory Integrator environment" on page 11
6. Copy the `config.properties` file. See "Copying the config.properties file from Documentum Content Server to the Security Directory Integrator environment" on page 12
7. Create the host entry. See "Creating an entry in the host file" on page 12

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.

Verifying the adapter installation
If the adapter is installed correctly, required components exist in the specified directories.

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.

Attribute mapping

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

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.

Copying DFC API JAR files from the Documentum Content Server to the Security Directory Integrator environment

You must install certain JAR files in the Security Directory Integrator environment to run the Documentum Content Server.

Before you begin

Copy the following list of DFC JAR files to the Security Directory Integrator environment:

- DmcRecords.jar
- dfc.jar
- dms-client-api.jar
- aspectjrt.jar
- certj.jar
- commons-lang-2.4.jar
- configservice-api.jar
- configservice-impl.jar
- cryptojFIPS.jar

Procedure

1. Copy the following list of DFC JAR files to the Security Directory Integrator environment:
   - DmcRecords.jar
   - dfc.jar
   - dms-client-api.jar
   - aspectjrt.jar
   - certj.jar
   - commons-lang-2.4.jar
   - configservice-api.jar
   - configservice-impl.jar
   - cryptojFIPS.jar
2. Copy the JAR files to ITDI_HOME/jars/3rd party/others folder from the Documentum installation directory/shared folder.

Copying the `config.properties` file from Documentum Content Server to the Security Directory Integrator environment

Procedure

1. Copy the `dfc.properties` file, from the Documentum Content Server to the workstation where your IBM Security Directory Integrator server is located. The file is located in the `Documentum/config` folder.
2. Copy the `dfc.properties` file to the `*ITDI_HOME*/timsol` folder or any other file path.

   Note: Mention the file path on the service form for dfc file path attribute to connect to underlying Documentum Content Server.

Creating an entry in the host file

Procedure

- Create an entry in the host files (`\windows\system32\drivers\etcfolder`) with the IP address of the Documentum Content Server:
  - If the Security Directory Integrator is running on a Windows workstation
  - If the Documentum Content Server is located on a different workstation than the Security Directory Integrator server.

Verifying the adapter installation

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

Use the following table to verify that you have installed and configured the TDI-based Documentum Server Adapter correctly in the Security Directory Integrator environment.

Table 3. Adapter components

Directory	Adapter components	Comments
`*ITDI_HOME*/jars/connectors`	`DocumentumConnector.jar`	None
`*ITDI_HOME*/jars/3rd party/others`	• `DmcRecords.jar` • `dfc.jar` • `dms-client-api.jar` • `aspectjrt.jar` • `certj.jar` • `commons-lang-2.4.jar` • `configservice-api.jar` • `configservice-impl.jar` • `cryptojFIPS.jar`	Documentum DFC API related JARs.
ITDI_HOME/timsol	`dfc.properties`	Documentum server properties file

If this installation is to upgrade a connector, 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 at *ITDI_Home**adapter solution directory*\logs.

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.

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

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.

Verifying the adapter installation
If the adapter is installed correctly, required components exist in the specified directories.

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.

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

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.

Verifying the adapter installation
If the adapter is installed correctly, required components exist in the specified directories.

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.

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

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.

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 Target Administration module. For more information, see *Attribute-to-permission mapping service* in the IBM Security Verify Governance Identity Manager 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.

Verifying the adapter installation
If the adapter is installed correctly, required components exist in the specified directories.

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.

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 14.

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.

Verifying the adapter installation
If the adapter is installed correctly, required components exist in the specified directories.

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.

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

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.

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`.

Documentum User ID

Specify the administrator ID that can log in to the resource and perform user management operations. Make sure that the administrator user has sufficient privileges to perform user management operations.

Documentum User Password

Specify the password for administrator user.

Docbase Name

Specify the Docbase Name on the service form which is configured at the time of the Documentum Content Server installation.

Dfc.properties file path

Mention the complete filepath of `dfc.properties` file which you have manually copied from the resource. For example: `-ITDI_HOME/timsol/dfc.properties` or `c:/documentum/dfc.properties`

Docbase Owner

Specify Docbase owner name on the service form under Docbase owner attribute. This is also mentioned in `dfcfull.properties` file on 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:

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 that are received from Identity server. For example, you can specify either of the following file paths to load the assembly lines from the `profiles` directory:

Windows operating systems

```
c:\Program Files\IBM\TDI\V7.1\profiles
```

UNIX and Linux® operating systems

```
/opt/IBM/TDI/V7.1/profiles
```

You must copy the assembly line files to the location that you specify for the AL FileSystem Path.

Server Host Name

Specify the managed resource on which you want to control the maximum connections with the Dispatcher property Max Connection Count.

Max Connection Count

Specify the maximum number of assembly lines that the Dispatcher can execute simultaneously for the service. If you enter `0` in the **Max Connection Count** field, the Dispatcher does not limit the number of assembly lines.

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.

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 Security Directory Integrator on which the adapter is deployed.

Dispatcher version
Specifies the version of the Dispatcher.

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

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

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

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

Verifying the adapter installation
If the adapter is installed correctly, required components exist in the specified directories.

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.

Attribute mapping

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

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.

Verifying the adapter installation
If the adapter is installed correctly, required components exist in the specified directories.

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.

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

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.

Verifying the adapter installation
If the adapter is installed correctly, required components exist in the specified directories.

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.

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

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.

Upgrading the connector

Procedure

- Before you upgrade the connector, verify the version of the connector:
  - If the connector version mentioned in the Release Notes is later than the existing version on your workstation, install the connector.
  - If the connector version mentioned in the Release Notes is earlier or the same as the existing version, do **not** install the connector.

  Note: Stop the dispatcher service before upgrading the connector and start it again after the upgrade is complete.

Related concepts

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

Related tasks

Upgrading the dispatcher

Upgrading the dispatcher

Procedure

- Before you upgrade the dispatcher, verify the version of the dispatcher:
  - If the Dispatcher version mentioned in the Release Notes is later than the existing version on your workstation, install the Dispatcher.
  - If the Dispatcher version mentioned in the Release Notes is the same or earlier than the existing version, do **not** install the Dispatcher.

  Note: Stop the Dispatcher service before upgrading the Dispatcher and start it again after the upgrade is complete.

Related concepts

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

Related tasks

Upgrading the connector

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.

Related tasks

Upgrading the connector
Upgrading the dispatcher

Chapter 5. Configuring

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

See the *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 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.

Creating a JAR file and importing the profile

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

About this task

If you are upgrading an existing adapter profile, the new adapter profile schema is not reflected immediately. You need to stop and start the Identity server to refresh the cache and the adapter schema. For more information about upgrading an existing adapter, see Chapter 4, "Upgrading," on page 25.

Procedure

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

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

   The **`jar`** command creates the `c:\temp\TDIDocuProfile.jar` directory.

2. Update the profile files.
3. Create a JAR file by using the files in the `\temp` directory by running the following commands:

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

4. Import the `TDIDocuProfile.jar.jar` file into the Identity server.
5. Restart the adapter service.

Password management for account restoration

When an account is restored from being previously suspended, you are prompted to provide a new password for the reinstated account. However, in some cases you might not want the be prompted for the password. The password requirement to restore an account falls into two categories:

- Allowed
- Required

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 Identity to forgo the new password requirement. You can set the adapter to require a new password if your organization requires passwords are reset when accounts are restored.

The adapter profile JAR file contains a `service.def` file In the `service.def` file, you can define whether a password is required as a new protocol option. When you import the adapter profile, and if an option is not specified, the adapter profile importer determines the correct restoration password behaviour from the `schema.dsml` file. Adapter profile components enable remote services to determine whether you discard a password that the user entered while multiple accounts on disparate resources are being restored. In this scenario, only some of th eaccounts that are 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 `<properties>...</properties>` section of 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 example, you are ensuring that you are not prompted for a password when an account is restored.

Note: Before you set the property **`PASSWORD_NOT_REQUIRED_ON_RESTORE`** to "true", ensure that the operating system supports restoring of an account without a password.

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.

Verifying the adapter installation
If the adapter is installed correctly, required components exist in the specified directories.

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.

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

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?

Related concepts

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.

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.

The following table contains warnings or errors message that might be displayed in the user interface when the adapter is installed on your system.

Table 4. Error messages

Error message	Possible cause	Corrective action

`DM_DOCBROKER_E_NO_DOCBROKERS]`
`error: "No DocBrokers are configured";`
`ERRORCODE: 100; NEXT: null`
	`dfc.properties` file is not specified correctly. It won't find the DocBase related information for connecting to the underlying resource.	Mention the proper file path for the `dfc.properties` file or ensure that you have provided proper and authenticated information.

`ERROR] [AGENTEXEC 5720] Detected during program initialization: Command Failed:`
`connect,`
`<server_name.docbase_name>,`
`<user>,`
`",,,try_native_first,`
`status: 0, with error message`
`[DFC_DOCBROKER_REQUEST_FAILED]`
`Request to Docbroker`
`"<docbroker_name>:<port>"`
`failed`
`[DM_SESSION_E_RPC_ERROR]error:`
`"Server communication failure`
	DFC trust-store wrong password.	Check all the entries in the `dfc.properties` file. Check that the password is correct.

Related concepts

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.

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 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.

Before you uninstall the adapter, inform your users that the adapter is unavailable. If you take the server offline, completed adapter requests might not be recovered when the server is back online.

Removing the adapter binaries or connector

Use this task to remove the connector file for the TDI-based Documentum Server Adapter.

About this task

The adapter installation process installs the Security Directory Integrator DocumentumConnector. You must remove the `DocumentumConnector.jar` file from the IBM Security Directory Integrator.

Procedure

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

Related concepts

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.

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.

Related tasks

Removing the adapter binaries or connector
Use this task to remove the connector file for the TDI-based Documentum Server Adapter.

Chapter 8. Reference

Reference information is organized to help you locate particular facts quickly, such as adapter attributes, registry settings, and environment variables.

Adapter attributes and object classes

Adapter attributes and object classes are required for customization, creating provisioning rules, and understanding what service/target attributes are supported by the adapter. The Identity server communicates with the adapter by using attributes, which are included in transmission packets that are sent over a network.

erTDIDocuAccount Object class

Table 5. Attributes for the erTDIDocuAccount object class

Attribute name and definition	Data type	Single-valued	Permissions	Required
eruid Specifies the Documentum Content Server user login ID.	String	Yes	RW	Yes
erTDIDocuOSName Specifies the user OS name of the user.	String	Yes	RW	Yes
erTDIDocuEmail Specifies the email address of the user.	String	Yes	RW	No
erTDIDocuObjectId r_object_id is the unique field serial number that is increased automatically. It is a read-only attribute.	String	Yes	R	No
erTDIDocuOSDomain Specifies the OS domain value of the user.	String	Yes	RW	No
erTDIDocuDescription Specifies the description of the documentum user.	String	Yes	RW	No
erTDIDocuIsGroup Determines if it is a group. If r_is_group = 0, it is not a group name. If r_is_group = 1, it is a group. It is a read-only attribute.	String	Yes	R	No
erTDIDocuDefaultFolder When you choose to create a user under a particular folder, Content Server would update the default_folder attribute of the dm_user to the updated folder path. By default, when a user is created, it is linked to `/Temp cabinet`.	String	Yes	RW	No
erPassword Specifies the password for the account.	String	Yes	RW	No

Table 5. Attributes for the erTDIDocuAccount object class (continued)

Attribute name and definition	Data type	Single-valued	Permissions	Required
erAccountStatus Specifies the status of the account during a suspend or restore operation.	Boolean	Yes	RW	No
erTDIDocuGroupDefault Specifies the default group name for that particular dm_user.	String	Yes	RW	No
erTDIDocuDBName Specifies the user database name for the Documentum user.	String	Yes	RW	No
erTDIDocuLDAPUser Specifies the `user_source` attribute of the user. It can be one of the following attributes: • LDAP • Inline Password • None	String	Yes	RW	No
erTDIDocuLastAccess Specifies the last account access date and time. It is a read-only attribute.	String	Yes	R	No
erTDIDocuACLName Specifies the ACL Name. For example: permissions set to the user. There are system ADs and user ADs. This value cannot be set to empty. Configure the server to choose the default ACL based on one of the following methods: • By User • By Object Type • By Default Folder	String	Yes	RW	No
erTDIDocuACLDomain Specifies the the ad_domain. This is set with the `acl_domain`. The owner name or user name falls under this attribute. This value cannot be set to empty.	String	Yes	RW	No
erTDIDocuASetName Specifies the alias set name of the Documentum user. Alias sets are lists of alias names paired with the alias ID attribute in `alias_set` table. Set `alias_set_id` attribute in the `dm_user` table, depending on the alias name set by the user.	String	Yes	RW	No

Table 5. Attributes for the erTDIDocuAccount object class (continued)

Attribute name and definition	Data type	Single-valued	Permissions	Required
erTDIDocuPrivileges Specifies the privileges set to the Documentum user. The following are the list of privileges: • None 0 • Create Type 1 • Create Cabinet 2 • Create Type + Create Cabinet 3 • Create Group 4 • Create Group + Create Type 5 • Create Group + Create Cabinet 6 • Create Group + Create Cabinet + Create Type 7 • Sysadmin 8 • Super User 16	String	Yes	RW	No
erTDIDocuCapabilities Specifies the client capabilities for the `dm_user` object.	String	Yes	RW	No
erTDIDocuUsrLnDomain Specifies the user login domain for the Documentum user account.	String	Yes	RW	No

erTDIRMIService object class

Table 6. Attributes for the erTDIRMIService object class

Attribute name and definition	Data type	Single-valued	Permissions	Required
erServiceName Specifies the name of the service.	String	Yes	RW	Yes
description Specifies the service description.	String	Yes	RW	No
erITDIurl Specifies the URL for the dispatcher.	String	Yes	RW	Yes
erTDIDocuDocbase Specifies the DocbaseName configured for the Documentum Content Server	String	Yes	RW	Yes
erTDIDocuDbOwner Specifies the Docbase owner name which is mentioned in the `dfcfull.properties` file.	String	Yes	RW	No

Table 6. Attributes for the erTDIRMIService object class (continued)

Attribute name and definition	**Data type**	**Single-valued**	**Permissions**	**Required**
erTDIDocuDbUser Specifies the Documentum user account ID. For example: Administrator account with superuser privileges.	String	Yes	RW	Yes
erTDIDocuDbPasswd Specifies the administrator account password for connecting to underlying resource.	String	Yes	RW	Yes
erTDIDocuDFCPath Specifies the path of the resource specified file. For example: `dfc.properties.file`.	String	Yes	RW	Yes
erTDIDocuALFileSystemPath Specifies a fully qualified file system path where the service assembly lines are found.	String	Yes	RW	No
erTDIDocuMaxConnectorCnt Specifies the maximum number of connections the Security Directory Integrator server can make for this service.	Integer	Yes	RW	No
erTDIDocuDisableALCache Specifies whether to cache the AL.	Boolean	Yes	RW	Yes

erTDIDocuGroup object class

Table 7. Attributes for the erTDIDocuGroup object class

Attribute name and definition	**Data type**	**Single-valued**	**Permissions**	**Required**
erTDIDocuNameGroup Specifies the name of the group.	String	Yes	R	Yes
erTDIDocuTypeGroup Specifies the type of the group.	String	Yes	R	Yes

erTDIDocuACL object class

Table 8. Attributes for the erTDIDocuACL object class

Attribute name and definition	**Data type**	**Single-valued**	**Permissions**	**Required**
erTDIDocuACLName Specifies the name of the ACL group.	String	Yes	R	Yes
erTDIDocuTypeGroup Specifies the type of the group.	String	Yes	R	Yes

erTDIDocuAliasGroup object class

Table 9. Attributes for the erTDIDocuAliasGroup object class

Attribute name and definition	Data type	Single-valued	Permissions	Required
erTDIDocuASetName Specifies the name of the alias group.	String	Yes	R	Yes
erTDIDocuTypeGroup Specifies the type of alias group	String	Yes	R	Yes

Index

IBM®