IBM Security Verify Identity
7.0

DB2 on z/OS Adapter Installation and Configuration Guide

Contents

Figures

Tables

Chapter 1. Overview

An adapter is an interface between a managed resource and the Identity server. The IBM® DB2 on z/OS adapter enables communication between the Identity server and the IBM DB2 on z/OS.

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

Features

The adapter automates several administrative and management tasks.

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

Related concepts

Architecture
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. There are two ways to configure the IBM DB2 on z/OS adapter. In a single server configuration, the adapter is installed on only one server. In a multiple server configuration, the adapter is installed on several different servers.

Architecture

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

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

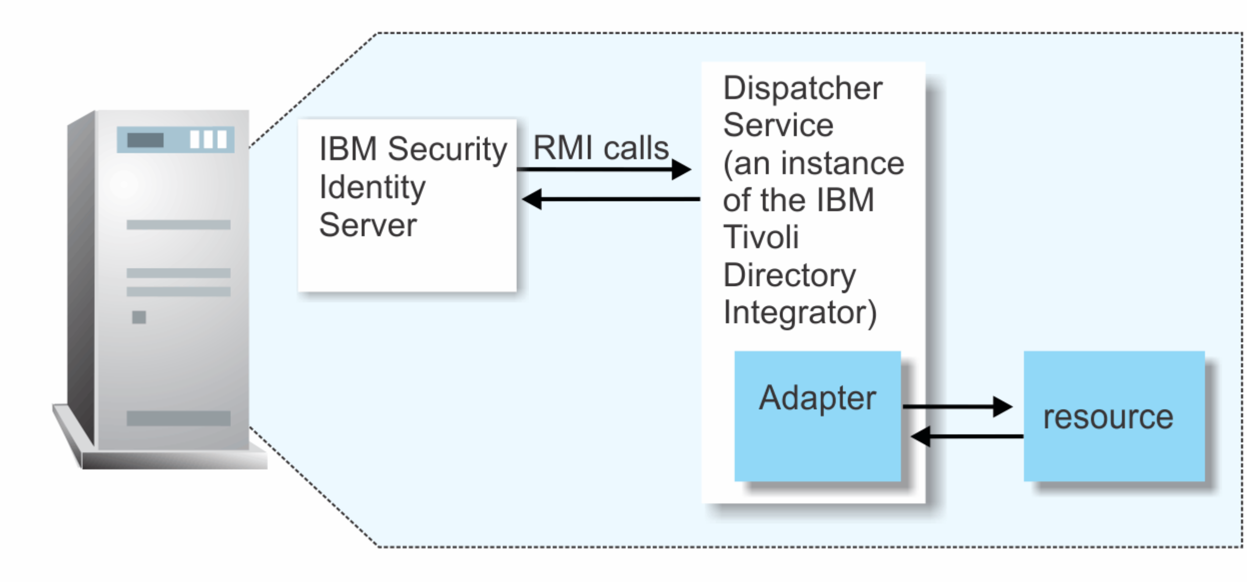
IBM Security Identity Server
RMI calls
Dispatcher Service (an instance of the IBM Tivoli Directory Integrator)
Adapter
resource

Figure 1. The architecture of the IBM DB2 on z/OS adapter

Related concepts

Features
The adapter automates several administrative and management tasks.

Supported configurations
The adapter supports both single and multiple server configurations. There are two ways to configure the IBM DB2 on z/OS adapter. In a single server configuration, the adapter is installed on only one server. In a multiple server configuration, the adapter is installed on several different servers.

Supported configurations

The adapter supports both single and multiple server configurations. There are two ways to configure the IBM DB2 on z/OS adapter. In a single server configuration, the adapter is installed on only one server. In a multiple server configuration, the adapter is installed on several different servers.

There are fundamental components in each environment:

- The Identity server
- The IBM Security Directory Integrator server
- The managed resource
- The adapter

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

Single server configuration

The Identity server, the Security Directory Integrator server, and the IBM DB2 on z/OS adapter are installed on one server to establish communication with the managed resource. The managed resource is installed on a different server as described Figure 2 on page 3.

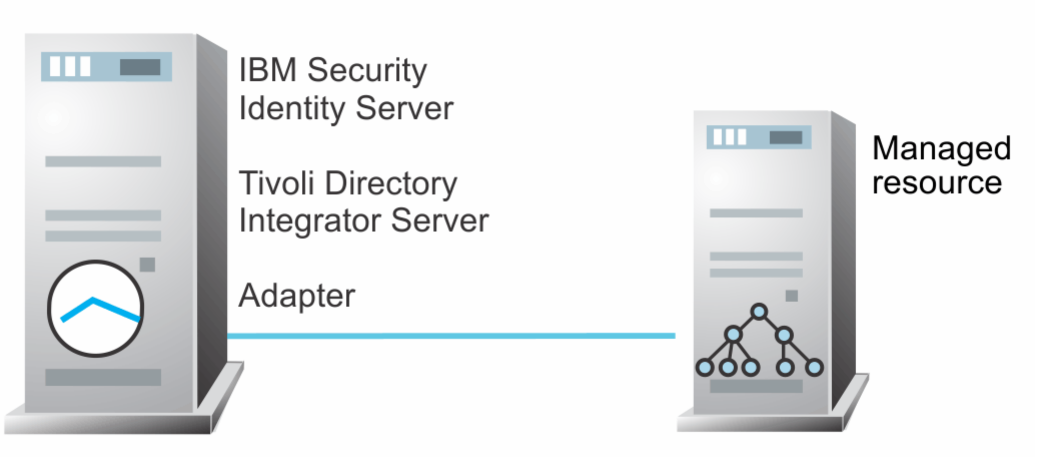

Figure 2. Example of a single server configuration

Multiple server configuration

In multiple server configuration, the Identity server, the Security Directory Integrator server, and the IBM DB2 on z/OS are installed on different servers. The Security Directory Integrator server and the IBM DB2 on z/OS adapter are installed on the same server as described in Figure 3 on page 3.

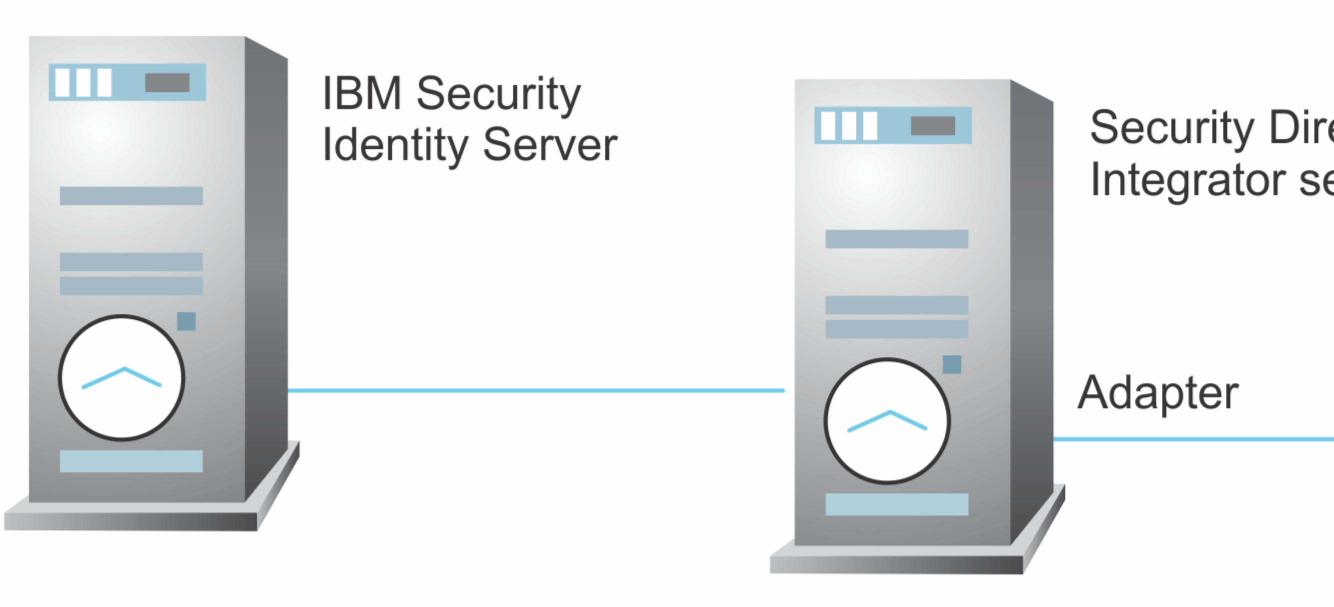

Figure 3. Example of multiple server configuration

Related concepts

Features
The adapter automates several administrative and management tasks.

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

Chapter 2. Planning

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

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

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

Pre-installation

Complete these tasks.

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

Installation

Complete these tasks.

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

Upgrade

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

Configuration

Complete these tasks.

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

Troubleshooting

See the following topics.

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

Uninstallation

Complete these tasks.

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

Reference

See the following topics.

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

Related concepts

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

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

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

Prerequisites

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

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

Ensure that you install the adapter on the same workstation as the 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
IBM DB2 on z/OS	A z system that runs IBM DB2® with one of the following versions: • IBM DB2, Version 10 for z/OS® • IBM DB2, Version 11 for z/OS

IBM DB2 JDBC Driver	• `db2jcc4.jar`
	• `db2jcc_license_cisuz.jar`
	Copy the JDBC drivers , which are included with the adapter package, to the following location:
	Windows
	`drive:\Program Files\IBM\TDI\TDI_VERSION\jars\3rdparty\IBM`
	Unix
	`/opt/IBM/TDI/TDI_VERSION/jars/3rdparty/IBM`
	Note: Delete the `db2jcc.jar`, if its present in the folder

Network Connectivity	Install the adapter on a workstation that can communicate with the IBM Security Verify Identity service through the TCP/IP network.
System Administrator Authority	To complete the adapter installation procedure, you must have system administrator authority.

Table 1. Prerequisites to install the adapter (continued)

Prerequisite	Description
Security Directory Integrator adapters solution directory	A Security Directory Integrator adapters solution directory is a Security Directory Integrator work directory for adapters. See the *Dispatcher Installation and Configuration Guide*.
IBM DB2 on z/OS Account, for example `db2admin`.	You must provide a IBM DB2 on z/OS account and password for every IBM DB2 on z/OS instance that the adapter manages. The IBM DB2 on z/OS account must have the following IBM DB2 on z/OS privileges: **SYSADM** System administrator. An ID with SYSADM authority that grants the privileges to the group ID.

Install the IBM DB2 on z/OS adapter and the appropriate IBM DB2 JDBC drivers on the same workstation as the Security Directory Integrator.

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 Identity 7.x
Follow this section when using the guide to install, configure, troubleshoot, or uninstall the adapter.

Software download
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 download

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

Go to IBM Passport Advantage.

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

Note:

You can also obtain additional adapter information from IBM Support.

Related concepts

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

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

Installation worksheet

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

Installation worksheet

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

Table 2. Required information to install the adapter

Required information	Description	Value

IBM Security Directory Integrator Home Directory	The *ITDI_HOME* directory contains the `jars/connectors` subdirectory. This subdirectory contains adapter JAR files.	IBM Security Directory Integrator can be automatically installed with your IBM Security Verify Identity product.
		The following are the default directory path that is used for Security Directory Integrator:
		Windows:
		`drive:\Program Files\IBM\TDI\TDI_VERSION`
		UNIX:
		`/opt/IBM/TDI/TDI_VERSION`

Adapters solution directory	When you install the dispatcher, the adapter prompts you to specify a file path for the adapters solution directory. If you do not specify a directory, the default directory is `timsol`.	**Windows:**
		`drive:\Program Files\IBM\TDI\TDI_VERSION\timsol`
		UNIX:
		`/opt/IBM/TDI/TDI_VERSION/timsol`

Related concepts

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

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

Software download
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 Dispatcher Installation Verification.

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

Installing the dispatcher

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

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

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

Related concepts

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

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

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

Related tasks

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

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

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

The Dispatcher must be installed.

About this task

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

Related concepts

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

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

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

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

Related tasks

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

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.

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.

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.

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 13.

About this task

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

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

Procedure

1. From the navigation tree, click **Manage Services**.

   The **Select a Service** page is displayed.
2. On the **Select a Service** page, click **Create**.

   The **Create a Service** wizard is displayed.
3. On the **Select the Type of Service** page, click **Search** to locate a business unit.

   The **Business Unit** page is displayed.
4. On the **Business Unit** page, complete these steps:

   a) Type information about the business unit in the **Search information** field.

   b) Select a business type from the **Search by** list, and then click **Search**.

      A list of business units that matches the search criteria is displayed.

      If the table contains multiple pages, you can do the following tasks:

      - Click the arrow to go to the next page.

  - Type the number of the page that you want to view and click **Go**.

  c) In the **Business Units** table, select business unit in which you want to create the service, and then click **OK**.

  The **Select the Type of Service** page is displayed, and the business unit that you specified is displayed in the **Business unit** field.

5. On the **Select the Type of Service** page, select a service type, and then click **Next**.

   If the table contains multiple pages, you can do the following tasks:

   - Click the arrow to go to the next page.
   - Type the number of the page that you want to view and click **Go**.

6. On either the **Service Information** or **General Information** page, specify the appropriate values for the service instance.

   The content of the **General Information** page depends on the type of service that you are creating. The creation of some services might require more steps.

7. To create a service with NTLM authentication, the administrator login is in the following format:

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

8. For NLTM authentication, select **Authentication** mode as 'Claims-Based Authentication.

9. On the **Dispatcher Attributes** page, specify information about the dispatcher attributes, and then click **Next** or **OK**.

   The **Dispatcher Attributes** page is displayed only for IBM Security Directory Integrator based services.

10. Optional: On the **Access Information** page, select the **Define an Access** check box to activate the access definition fields. Select the type of access you want to enable.

    Specify the expected access information and any other optional information such as description, search terms, more information, or badges.

11. On the **Status and Information** page, view information about the adapter and managed resource, and then click **Next** or **Finish**.

    The adapter must be running to obtain the information.

12. On the **Configure Policy** page, select a provisioning policy option, and then click **Next** or **Finish**.

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

    Note: If you are creating a service for an identity feed, the **Configure Policy** page is not displayed.

13. Optional: On the **Reconcile Supporting Data** page, either do an immediate reconciliation for the service, or schedule a supporting data reconciliation, and then click **Finish**.

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

    The **supporting data only** reconciliation option retrieves only the supporting data for accounts. The supporting data includes groups that are defined on the service. The type of supporting data is defined in the adapter guide.

14. Optional: On the **Service Information** or **General Information** page, click **Test Connection** to validate that the data in the fields is correct, and then click **Next** or **Finish**.

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

Results

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

Related concepts

Installing the dispatcher

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

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

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

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

Related tasks

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

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

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 IBM DB2 on z/OS Connection 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.

Tivoli® 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`.

IBM DB2 on z/OS Server Host
Specify the host workstation on which the IBM DB2 on z/OS server is running.

IBM DB2 on z/OS Server Port
Specify the TCP port on which the IBM DB2 on z/OS server is running. You can specify 50000 to use the default DB2 port.

IBM DB2 on z/OS Database Name
Specify the database name of the IBM DB2 on z/OS database that you want to manage, for example SAMPLE.

IBM DB2 on z/OS Administration User Account
Specify the name of the user who has access to the IBM DB2 on z/OS resource and who can do administrative operations.

IBM DB2 on z/OS Administration User Password
Specify the password for the user.

Owner
Optionally, specify a user as a service owner.

Service Prerequisite
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, delete, and test operations are not cached.

AL File System 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.

You can specify the following file path to load the assembly lines from the profiles directory of the Windows operating system: `c:\Files\IBM\TDI\V7.1\profiles`.

Alternatively, you can specify the following file path to load the assembly lines from the profiles directory of the UNIX and Linux operating system: system: `/opt/IBM/TDI/V7.1/profiles`.

Max Connection Count
Specify the maximum number of assembly lines that the dispatcher can run simultaneously for the service. Enter `10` if you want the dispatcher to run a maximum of 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 run simultaneously for the service.

On the Status and information tab
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 is 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. Verify parameters such as the work station name or the IP address of the managed resource and the port.

Related concepts

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

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

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

Related tasks

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

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

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.

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.

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 dispatcher

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 the 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.

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 concepts

Upgrading the dispatcher
Before you upgrade the dispatcher, verify the version of 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 *IBM Security Dispatcher Installation and Configuration Guide* for more configuration options such as:

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

Customizing the adapter profile

To customize the adapter profile, you must modify the IBM DB2 on z/OS adapter JAR file. You might customize the adapter profile to change the account form or the service form.

About this task

You can also use the Form Designer or the `CustomLabels.properties` file to change the labels on the forms. Each adapter has a `CustomLabels.properties` file for that adapter.

The JAR file is included in the IBM DB2 on z/OS adapter compressed file that you downloaded from the IBM website. The IBM DB2 on z/OS JAR file and the files that are contained in the JAR file vary depending on your operating system.

Note: You cannot modify the schema for this adapter. You cannot add or delete attributes from the schema.

The adapter JAR file includes the following files:

- `CustomLabels.properties`
- `erZDB2Account.xml`
- `erZDB2Service.xml`
- `schema.dsml`
- `service.def`
- `ZDB2AddUserAL.xml`
- `ZDB2DeleteUserAL.xml`
- `ZDB2ModifyUserAL.xml`
- `ZDB2SearchUserAL.xml`
- `ZDB2TestAL.xml`

Procedure

- To edit the JAR file, take these steps:
  a) Log on to the workstation where the IBM DB2 on z/OS adapter is installed.
  b) On the **Start** menu, click **Programs → Accessories → Command Prompt**.
  c) Copy the JAR file into a temporary directory.
  d) Extract the contents of the JAR file into the temporary directory by running the following command.

The following example applies to the IBM DB2 on z/OS adapter profile. Type the name of the JAR file for your operating system.

```
cd c:\temp
jar -xvf ZDB2AdapterProfile.jar
```

The **jar** command extracts the files into the directory.

e) Edit the file that you want to change

After you edit the file, you must import the file into the Identity server for the changes to take effect.

- To import the file, take these steps:

a) Create a JAR file by using the files in the `\temp` directory.

Run the following commands:

```
cd c:\temp
jar -cvf ZDB2AdapterProfile.jar ZDB2AdapterProfile
```

b) Import the JAR file into the IBM Security Verify Identity application server.

c) Stop and start the Identity server

d) Restart the adapter service.

Related tasks

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.

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.

Related tasks

Customizing the adapter profile
To customize the adapter profile, you must modify the IBM DB2 on z/OS adapter JAR file. You might customize the adapter profile to change the account form or the service form.

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.

A warning or error might be displayed in the user interface to provide information that you must know about the adapter or about an error. Table 3 on page 29 contains warnings or errors that might be displayed in the user interface if the IBM DB2 on z/OS adapter is installed on your system.

Table 3. Warning and error messages

Message code	Warning or error message	Remedial action
CTGIMT001E	The following error occurred. Error: Either the IBM DB2 on z/OS service name is incorrect or the service is not up.	Ensure that the IBM DB2 on z/OS service name given on IBM Security Verify Identity service form is running.
CTGIMT001E	The following error occurred. Error: Either the IBM DB2 on z/OS host or port is incorrect.	Verify that the host workstation name or the port for the IBM DB2 on z/OS service is correctly specified.
CTGIMT002E	The login credential is missing or incorrect.	Verify that you provided correct login credential on service form.
CTGIMT001E	The following error occurred. Error: No suitable JDBC driver found.	Ensure that the correct version of the JDBC driver is copied onto the workstation where the adapter is installed. Ensure that the path for the driver is included in the system CLASSPATH variable.
CTGIMT600E	An error occurred while establishing communication with the IBM Security Directory Integrator server.	IBM Security Verify Identity cannot establish a connection with IBM Security Directory Integrator. To fix this problem, ensure that: • IBM Security Directory Integrator is running. • The URL specified on the service form for the IBM Security Directory Integrator is correct.
CTGIMT003E	The account already exists.	Use a different name for the user to be added.
CTGIMT015E	An error occurred while deleting the *Account_Name* account because the account does not exist.	The user you trying to delete does not exist. Ensure that you are deleting only an existing account.

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.

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.

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

As part of the adapter implementation, a dedicated account that allows IBM Security Verify Identity to access the IBM DB2 on z/OS is created on the IBM DB2 on z/OS.

The adapter consists of files and directories that are owned by the IBM Security Verify Identity account. These files establish communication with the Identity server.

Attribute descriptions

The Identity server communicates with the adapter by using attributes, which are included in transmission packets that are sent over a network.

The combination of attributes depends on the type of action that the IBM Security Verify Identity server requests from the adapter.

Table 4 on page 33 lists the account form attributes that the adapter uses.

Table 4. Attributes, descriptions, and corresponding data types

Attribute	Directory server attribute	Description	Data format
Administration User Account	erRmiZDBAdminName	Specify the user ID that is used to connect to the IBM DB2 on z/OS. The value of this key must be the administrator user of the Cataloged database. Administration User Account is the required field.	String
Administration User Password	erServicePwd1	Specify the password for the user ID that is used to connect to the IBM DB2 on z/OS. The value of this key must be the password of the administrator user of the Cataloged database. Administration User Password is the required field.	String
System privileges	erRmiZOSSysPriv	Specifies the list of system privileges.	String
System privileges with grant option	erRmiZOSSysPrivGrant	Specifies the list of system privileges with grant option	String

Table 4. Attributes, descriptions, and corresponding data types (continued)

Attribute	Directory server attribute	Description	Data format
PrivCreateinSchema	erRmiZDBPrivCreateinSchema	Specifies all schemas on which the privilege to create objects in the schema is granted to the user. It is multivalued.	String
erRmiZDBPrivWGrCreateinSchema	erRmiZDBPrivWGrCreateinSchema	Specifies all schemas on which the privilege to create objects in the schema is granted to the user. It is multivalued.	String
PrivAlterinSchema	erRmiZDBPrivAlterinSchema	Specifies all schemas on which the privilege to alter objects in the schema is granted to the user. It is multivalued.	String
PrivWGrAlterinSchema	erRmiZDBPrivWGrAlterinSchema	Specifies all schemas on which the privilege to alter objects in the schema with grant option is granted to the user. It is multivalued	String
ZDBPrivDropinSchema	erRmiZDBPrivDropinSchema	Specifies all schemas on which the privilege to drop objects in the schema is granted to the user. It is multivalued.	String
ZDBPrivWGrDropinSchema	erRmiZDBPrivWGrDropinSchema	Specifies all schemas on which the privilege to drop objects in the schema with grant option is granted to the user. It is multivalued.	String
PrivSelectTab	erRmiZDBPrivSelectTab	Specifies all tables on which the select privilege is granted to the user. It is multivalued.	String
PrivWGrSelectTab	erRmiZDBPrivWGrSelectTab	Specifies all tables on which the select privilege with grant option is granted to the user. It is multivalued.	String

Table 4. Attributes, descriptions, and corresponding data types (continued)

Attribute	Directory server attribute	Description	Data format
PrivInsertTab	erRmiZDBPrivInsertTab	Specifies all tables on which the insert privilege is granted to the user. It is multivalued.	String
PrivWFRInsertTab	erRmiZDBPrivWGrInsertTab	Specifies all tables on which the Insert privilege with grant option is granted to the user. It is multivalued.	String
PrivUpdateTab	erRmiZDBPrivUpdateTab	Specifies all tables on which the Update privilege is granted to the user. It is multivalued.	String
PrivWGrUpdateTab	erRmiZDBPrivWGrUpdateTab	Specifies all tables on which the Update privilege with grant option is granted to the user. It is multivalued.	String
PrivDeleteTab	erRmiZDBPrivDeleteTab	Specifies all tables on which the Delete privilege is granted to the user. It is multivalued.	String
PrivWGrDeleteTab	erRmiZDBPrivWGrDeleteTab	Specifies all tables on which the Delete privilege with grant option is granted to the user. It is multivalued.	String
PrivAlterTab	erRmiZDBPrivAlterTab	Specifies all tables on which the Alter privilege is granted to the user. It is multivalued.	String
PrivWGrAlterTab	erRmiZDBPrivWGrAlterTab	Specifies all tables on which the Alter privilege with grant option is granted to the user. It is multivalued.	String
PrivIndexTab	erRmiZDBPrivIndexTab	Specifies all tables on which the Index privilege is granted to the user. It is multivalued.	String

Table 4. Attributes, descriptions, and corresponding data types (continued)

Attribute	Directory server attribute	Description	Data format
PrivWGrIndexTab	erRmiZDBPrivWGrIndexTab	Specifies all tables on which the Index privilege with grant option is granted to the user. It is multivalued.	String
PrivRefTab	erRmiZDBPrivRefTab	Specifies all tables on which the References privilege is granted to the user. It is multivalued.	String
PrivWGrRefTab	erRmiZDBPrivWGrRefTab	Specifies all tables on which the References privilege with grant option is granted to the user. It is multivalued.	String
PrivUseTabSpace	erRmiZDBPrivUseTabSpace	Specifies all schemas on which the use privilege is granted to the user. It is multivalued.	String
PrivWGrUseTabSpace	erRmiZDBPrivWGrUseTabSpace	Specifies all schemas on which the use privilege with grant option is granted to the user. It is multivalued.	String
PrivSelectView	erRmiZDBPrivSelectView	Specifies all views on which the select privilege is granted to the user. It is multivalued.	String
PrivWGrSelectView	erRmiZDBPrivWGrSelectView	Specifies all views on which the select privilege with grant option is granted to the user. It is multivalued.	String
PrivInsertView	erRmiZDBPrivInsertView	Specifies all views on which the Insert privilege is granted to the user. It is multivalued.	String
PrivWGrInsertView	erRmiZDBPrivWGrInsertView	Specifies all views on which the Insert privilege with grant option is granted to the user. It is multivalued.	String

Table 4. Attributes, descriptions, and corresponding data types (continued)

Attribute	Directory server attribute	Description	Data format
PrivUpdateView	erRmiZDBPrivUpdateView	Specifies all views on which the Update privilege is granted to the user. It is multivalued.	String
PrivWGrUpdateView	erRmiZDBPrivWGrUpdateView	Specifies all views on which the Update privilege with grant option is granted to the user. It is multivalued.	String
PrivVwDeleteView	erRmiZDBPrivVwDeleteView	Specifies all views on which the Delete privilege is granted to the user. It is multivalued.	String
PrivWgrVwDeleteView	erRmiZDBPrivWGrVwDeleteView	Specifies all views on which the Delete privilege with grant option is granted to the user. It is multivalued.	String
DBCreateTab	erRmiDBCreateTab	Specifies all Databases on which the Create Tab privilege is granted to the user. It is multivalued.	String
DBWGrCreateTab	erRmiDBWGrCreateTab	Specifies all Databases on which the Create Tab privilege with grant option is granted to the user. It is multivalued.	String
DBCreateTs	erRmiDBCreateTs	Specifies all Databases on which the Creates privilege is granted to the user. It is multivalued.	String
DBWGrCreateTs	erRmiDBWGrCreateTs	Specifies all Databases on which the CreateTs privilege with grant option is granted to the user. It is multivalued.	String
DBDrop	erRmiDBDrop	Specifies all Databases on which the dropdb privilege is granted to the user. It is multivalued.	String

Table 4. Attributes, descriptions, and corresponding data types (continued)

Attribute	Directory server attribute	Description	Data format
DBWgrDrop	erRmiDBWgrDrop	Specifies all Databases on which the dropdb privilege with grant option is granted to the user. It is multivalued.	String
DBDisplayDb	erRmiDBDisplayDb	Specifies all Databases on which the displaydb privilege is granted to the user. It is multivalued.	String
DBWgrDisplayDb	erRmiDBWgrDisplayDb	Specifies all Databases on which the displaydb privilege with grant option is granted to the user. It is multivalued.	String
DbImagCopy	erRmidbImagCopy	Specifies all Databases on which the imagcopy privilege is granted to the user. It is multivalued.	String
DbWgrImagCopy	erRmidbWgrImagCopy	Specifies all Databases on which the imagcopy privilege with grant option is granted to the user. It is multivalued.	String
DBLoad	erRmiDBLoad	Specifies all Databases on which the load privilege is granted to the user. It is multivalued.	String
DBWgrLoad	erRmiDBWgrLoad	Specifies all Databases on which the load privilege with grant option is granted to the user. It is multivalued.	String
DBRecoverDb	erRmiDBRecoverDb	Specifies all Databases on which the recover privilege is granted to the user. It is multivalued.	String

Table 4. Attributes, descriptions, and corresponding data types (continued)			
Attribute	**Directory server attribute**	**Description**	**Data format**
DBWgrRecoverDb	erRmiDBWgrRecoverDb	Specifies all Databases on which the recover privilege with grant option is granted to the user. It is multivalued.	String
DBReorg	erRmiDBReorg	Specifies all Databases on which the reorg privilege is granted to the user. It is multivalued.	String
DBWgrReorg	erRmiDBWgrReorg	Specifies all Databases on which the reorg privilege with grant option is granted to the user. It is multivalued.	String
DBStartDb	erRmiDBStartDb	Specifies all Databases on which the startdb privilege is granted to theu ser. It is multivalued.	String
DBWgrStartDb	erRmiDBWgrStartDb	Specifies all Databases on which the startdb privilege with grant option is granted to the user. It is multivalued.	String
DBRepair	erRmiDBRepair	Specifies all Databases on which the repair privilege is granted to the user. It is multivalued.	String
DBWgrRepair	erRmiDBWgrRepair	Specifies all Databases on which the repair privilege with grant option is granted to the user. It is multivalued.	String
DBStats	erRmiDBStats	Specifies all Databases on which the stats privilege is granted to the user. It is multivalued.	String

Table 4. Attributes, descriptions, and corresponding data types (continued)

Attribute	**Directory server attribute**	**Description**	**Data format**
DBWgrStats	erRmiDBWgrStats	Specifies all Databases on which the stats privilege with grant option is granted to the user. It is multivalued.	String
DBStopdb	erRmiDBStopdb	Specifies all Databases on which the stopdb privilege is granted to the user. It is multivalued.	String
DBWgrStopdb	erRmiDBWgrStopdb	Specifies all Databases on which the stopdb privilege with grant option is granted to the user. It is multivalued.	String
DBDbadm	erRmiDBDbadm	Specifies all Databases on which the dbadm privilege is granted to the user. It is multivalued.	String
DBWgrDbadm	erRmiDBWgrDbadm	Specifies all Databases on which the dbadm privilege with grant option is granted to the user. It is multivalued.	String
DBCtrl	erRmiDBCtrl	Specifies all Databases on which the dbctrl privilege is granted to the user. It is multivalued.	String
DBWgrCtrl	erRmiDBWgrCtrl	Specifies all Databases on which the dbctrl privilege with grant option is granted to the user. It is multivalued.	String
DBMaint	erRmiDBMaint	Specifies all Databases on which the dbmaint privilege is granted to the user. It is multivalued.	String

Table 4. Attributes, descriptions, and corresponding data types (continued)			
Attribute	**Directory server attribute**	**Description**	**Data format**
DBWgrMaint	erRmiDBWgrMaint	Specifies all Databases on which the dbmaint privilege with grant option is granted to the user. It is multivalued.	String

Related reference

Adapter attributes by action

The following lists describe typical adapter actions that are organized by their functional transaction group. The lists include more information about required and optional attributes that are sent to the adapter to complete that action.

Adapter attributes by action

The following lists describe typical adapter actions that are organized by their functional transaction group. The lists include more information about required and optional attributes that are sent to the adapter to complete that action.

Related reference

Attribute descriptions

The Identity server communicates with the adapter by using attributes, which are included in transmission packets that are sent over a network.

Database login add

A database login add is a request to create a user account with the specified attributes.

Table 5. Add request attributes

Required attribute	Optional attribute	
eruid	erRmiZOSSysPrivGrant	erRmiDBCreateTab
erRmiZOSSysPriv	erRmiZDBPrivCreateinSchema	erRmiDBWGrCreateTab
	erRmiZDBPrivWGrCreateinSchema	erRmiDBCreateTs
	erRmiZDBPrivAlterinSchema	erRmiDBWGrCreateTs
	erRmiZDBPrivWGrAlterinSchema	erRmiDBDrop
	erRmiZDBPrivDropinSchema	erRmiDBWgrDrop
	erRmiZDBPrivWGrDropinSchema	erRmiDBDisplayDb
	erRmiZDBPrivSelectTab	erRmiDBWgrDisplayDb
	erRmiZDBPrivWGrSelectTab	erRmidbImagCopy
	erRmiZDBPrivInsertTab	erRmidbWgrImagCopy
	erRmiZDBPrivWGrInsertTab	erRmiDBLoad
	erRmiZDBPrivUpdateTab	erRmiDBWgrLoad
	erRmiZDBPrivWGrUpdateTab	erRmiDBRecoverDb
	erRmiZDBPrivDeleteTab	erRmiDBWgrRecoverDb
	erRmiZDBPrivWGrDeleteTab	erRmiDBReorg
	erRmiZDBPrivAlterTab	erRmiDBWgrReorg
	erRmiZDBPrivWGrAlterTab	erRmiDBStartDb
	erRmiZDBPrivIndexTab	erRmiDBWgrStartDb
	erRmiZDBPrivWGrIndexTab	erRmiDBRepair
	erRmiZDBPrivRefTab	erRmiDBWgrRepair
	erRmiZDBPrivWGrRefTab	erRmiDBStats
	erRmiZDBPrivUseTabSpace	erRmiDBWgrStats
	erRmiZDBPrivWGrUseTabSpace	erRmiDBStopdb
	erRmiZDBPrivSelectView	erRmiDBWgrStopdb
	erRmiZDBPrivWGrSelectView	erRmiDBDbadm
	erRmiZDBPrivInsertView	erRmiDBWgrDbadm
	erRmiZDBPrivWGrInsertView	erRmiDBCtrl
	erRmiZDBPrivUpdateView	erRmiDBWgrCtrl
	erRmiZDBPrivWGrUpdateView	erRmiDBMaint
	erRmiZDBPrivVwDeleteView	erRmiDBWgrMaint
	erRmiZDBPrivWGrVwDeleteView	

Database login change

A database login change is a request to change one or more attributes for the specified users.

Table 6. Change request attributes

Required attribute	Optional attribute	
eruid	erRmiZOSSysPrivGrant erRmiZOSSysPriv erRmiZDBPrivCreateinSchema erRmiZDBPrivWGrCreateinSchema erRmiZDBPrivAlterinSchema erRmiZDBPrivWGrAlterinSchema erRmiZDBPrivDropinSchema erRmiZDBPrivWGrDropinSchema erRmiZDBPrivSelectTab erRmiZDBPrivWGrSelectTab erRmiZDBPrivInsertTab erRmiZDBPrivWGrInsertTab erRmiZDBPrivUpdateTab erRmiZDBPrivWGrUpdateTab erRmiZDBPrivDeleteTab erRmiZDBPrivWGrDeleteTab erRmiZDBPrivAlterTab erRmiZDBPrivWGrAlterTab erRmiZDBPrivIndexTab erRmiZDBPrivWGrIndexTab erRmiZDBPrivRefTab erRmiZDBPrivWGrRefTab erRmiZDBPrivUseTabSpace erRmiZDBPrivWGrUseTabSpace erRmiZDBPrivSelectView erRmiZDBPrivWGrSelectView erRmiZDBPrivInsertView erRmiZDBPrivWGrInsertView erRmiZDBPrivUpdateView erRmiZDBPrivWGrUpdateView erRmiZDBPrivVwDeleteView erRmiZDBPrivWGrVwDeleteView	erRmiDBCreateTab erRmiDBWGrCreateTab erRmiDBCreateTs erRmiDBWGrCreateTs erRmiDBDrop erRmiDBWgrDrop erRmiDBDisplayDb erRmiDBWgrDisplayDb erRmidbImagCopy erRmidbWgrImagCopy erRmiDBLoad erRmiDBWgrLoad erRmiDBRecoverDb erRmiDBWgrRecoverDb erRmiDBReorg erRmiDBWgrReorg erRmiDBStartDb erRmiDBWgrStartDb erRmiDBRepair erRmiDBWgrRepair erRmiDBStats erRmiDBWgrStats erRmiDBStopdb erRmiDBWgrStopdb erRmiDBDbadm erRmiDBWgrDbadm erRmiDBCtrl erRmiDBWgrCtrl erRmiDBMaint erRmiDBWgrMaint

Database login delete

A database login delete is a request to remove the specified user from the directory.

Table 7. Delete request attributes

Required attribute	Optional attribute
erUid	None

Database login suspend

A database login suspend is a request to disable a user account.

The user is not removed. User attributes are not modified.

Table 8. Suspend request attributes

Required attribute	Optional attribute
erUid erAccountStatus	None

Database login restore

A database login restore is a request to activate a user account that was previously suspended.

After an account is restored, the user can access the system by using the same attributes as the ones before the Suspend function was called.

Table 9. Restore attributes

Required attribute	Optional attribute
erUid erAccountStatus	None

Ping

Use Ping to verify connection between the adapter and the Identity server. Ping does not require any variables.

Table 10. Ping attributes

Required attribute	Optional attribute
None	None

Reconciliation

The reconciliation function synchronizes user account information between IBM Security Verify Identity and the adapter.

Table 11. Reconciliation attributes

Attribute
All supported attributes

Index

IBM®