IBM Security Verify Identity
7.0

MySQL Adapter Installation and Configuration Guide

Contents

Tables v

Chapter 1. Overview 1
- Features 1
- Architecture 1

Chapter 2. Planning 3
- Prerequisites 3
- Software downloads 4
- Installation worksheet 4

Chapter 3. Installing 7
- Installing the dispatcher 7
- Installing the adapter binaries or connector 8
- Restarting the adapter service 9
- Importing the adapter profile 9
- Creating an adapter service/target 11
- Service/Target form details 13
- Installing the adapter language package 15
- Verifying that the adapter is working correctly 16

Chapter 4. Upgrading 17
- Upgrading the dispatcher 17
- Upgrading the adapter profile 17

Chapter 5. Configuring 19
- Customizing the adapter profile 19
- Editing adapter profiles on the UNIX or Linux operating system 20

Chapter 6. Troubleshooting 21
- Techniques for troubleshooting problems 21
- Error messages and problem solving 23

Chapter 7. Uninstalling 25
- Deleting the adapter profile 25

Chapter 8. Reference 27
- Adapter attributes 27
- Adapter attributes by operations 28
  - System Login Add 28
  - System Login Change 28
  - System Login Suspend 28
  - System Login Restore 29
  - Test 29
  - Reconciliation 29
- Adapter configuration properties 29
- Special attributes 29

Index..... 31

Tables

1. Prerequisites to install the adapter....3

2. Required information to install the adapter....4

3. Required privileges and their descriptions....13

4. Warning and error messages 23

5. Supported Account attributes....27

6. Supported Role attributes....27

7. Supported Schema Privileges Attributes 27

8. Supported Schema Privileges Attributes 28

9. Supported object classes....28

10. Add request attributes.... 28

11. Change request attributes.... 28

12. Suspend request attributes.... 28

13. Restore attributes.... 29

14. Test attributes.... 29

15. Reconciliation request attributes.... 29

Chapter 1. Overview

An adapter is an interface between a managed resource and the Identity server. The MySQL Adapter enables communication between the Identity server and the MySQL.

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 such as roles
- Adding and modifying user accounts
- Modifying user account attributes
- Modifying user account password
- Suspending, and restoring user accounts

Related concepts

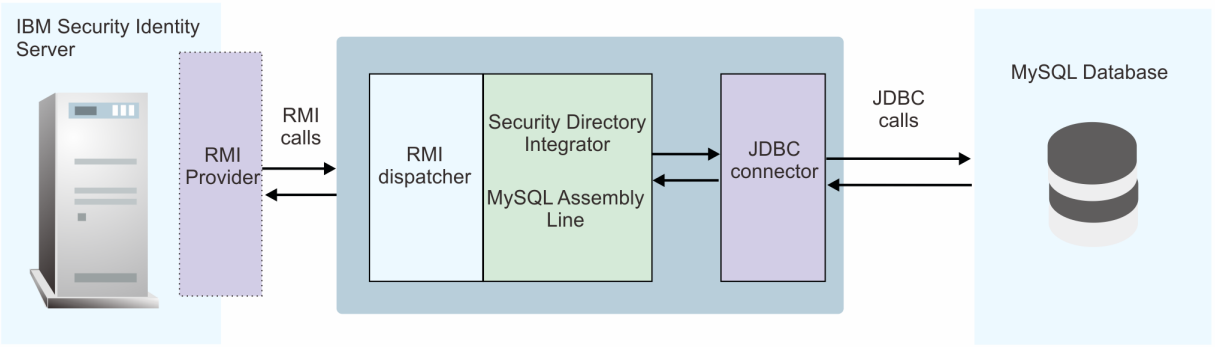
Architecture

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

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



Related concepts

Features

The adapter automates several administrative and management tasks.

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.

Prerequisites

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

Table 1 on page 3 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 + Fix Pack 4 See the adapter release notes for the latest information on supported component versions.
Identity server	The following servers are supported: • Identity server Version 10.0 • Identity server Version 10.0 • Identity server Version 10.0 See the adapter release notes for the latest information on supported component versions.
MySQL Server	IBM MySQL Server 8.0.19
MySQL JDBC Driver	JDBC Driver **Note:** The driver file name is: • `mysql-connector-java-5.1.48.jar`
IBM Security Directory Integrator adapters solution directory	The IBM Security Directory Integrator adapters solution directory is a IBM Security Directory Integrator work directory for adapters. See the *Dispatcher Installation and Configuration Guide*.
System administrator authority	You must have system administrator authority to complete the adapter installation procedure.

Install the MySQL Adapter and the appropriate MySQL JDBC drivers on the same workstation as the IBM Security Directory Integrator.

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

Related concepts

Software downloads

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

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

Software downloads

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

Go to IBM Passport Advantage.

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

Note:

You can also obtain additional adapter information from IBM Support.

Related concepts

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 which contains the files for the adapters.	If IBM Security Directory Integrator is automatically installed with your IBM Security Verify Identity product, the default directory path for IBM Security Directory Integrator is as follows: Windows: • *drive*`\Program Files \IBM\TDI\V7.2` UNIX: • `/opt/IBM/TDI/V7.2`

Table 2. Required information to install the adapter (continued)		
Required information	**Description**	**Value**
Adapters solution directory	When you install the dispatcher, the adapter prompts you to specify a file path for the adapters solution directory. For more information about the solution directory, see the *Dispatcher Installation and Configuration Guide*.	The default solution directory is at: Windows • *drive*\Program Files \IBM\TDI\V7.2\ UNIX: • /opt/IBM/TDI/V7.2/

Related concepts

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

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

Chapter 3. Installing

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

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

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

Installing the dispatcher

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

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

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

Related concepts

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

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

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

Related tasks

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

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

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

Verifying that the adapter is working correctly

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

Installing the adapter binaries or connector

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

Before you begin

- The Dispatcher must be installed.
- Ensure that your sites meets the prerequisite requirements. See "Prerequisites" on page 3.

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*..

Procedure

1. Download `mysql-connector-java-5.1.48.jar` from MySQL Connector/J 5.1.48.
2. Copy the MySQL JDBC driver to the `ITDI_HOME/jars/3rdparty/others` directory.
   For example: `mysql-connector-java-5.1.48.jar`
3. Restart the adapter service.

Related concepts

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

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

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

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

Related tasks

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

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

Verifying that the adapter is working correctly

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

Restarting the adapter service

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

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

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

Related concepts

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

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

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

Related tasks

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

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

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

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

Importing the adapter profile

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

Before you begin

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

About this task

Service definition files are also called adapter profile files.

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

Procedure

1. Log on to the Identity server by using an account that has the authority to perform administrative tasks.
2. From the navigation tree, select **Configure System** > **Manage Service Types**.

   The **Manage Service Types** page is displayed.
3. On the **Manage Service Types** page, click **Import**.

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

Results

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

What to do next

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

Related concepts

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

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

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

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

Related tasks

Installing the adapter binaries or connector

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

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

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

Creating an adapter service/target

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

Before you begin

Complete "Importing the adapter profile" on page 9.

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. 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.
8. 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.
9. 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.
10. 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.
11. 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.
12. Optional: On the **Service Information** or **General Information** page, click **Test Connection** to validate that the data in the fields is correct, and then click **Next** or **Finish**.

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

Results

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

Related concepts

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

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

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

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

Related tasks

Installing the adapter binaries or connector

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

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

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

Service/Target form details

Complete the service/target form fields.

You must create a user account for the adapter on the managed resource. The accounts must be able to remotely connect to the MySQL and must have sufficient privileges to administer MySQL users.

Table 3. Required privileges and their descriptions

Privilege	Description
CREATEUSER	Create root user
GRANTALLPRIVILEGES	GRANT ALL PRIVILEGES ON *.* TO 'USERNAME'@'%' IDENTIFIED BY 'PASSWORD' WITH GRANT OPTION;

On the MySQL 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`.

MySQL Server Host
Specify the host IP or name on which the MySQL server is running.

MySQL Server Port
Specify the TCP port on which the MySQL server is running. You can specify 5432 to use the default MySQL port.

MySQL Database Name
Specify the database name of the MySQL database that you want to manage, for example POSTGRES.

MySQL Administration User Account
Specify the name of the user who has access to the MySQL resource and who can do administrative operations.

MySQL Administration User Password
Specify the password for the user.

On the Dispatcher Attributes tab:

Assembly Line File System Path

Optionally, you can specify the path from where the Dispatcher loads the assembly lines. If you do not specify a file path, the Dispatcher loads the default assembly lines from the adapter's profile

For example:

Windows operating system:
```
C:\Program Files\IBM\TDI\V7.2\profiles
```

UNIX and Linux operating system
```
/opt/IBM/TDI/V7.2/profiles
```

Disable Assembly Line Caching
Select the check box to disable the assembly line caching in the dispatcher for the service. When disabled, the assembly lines for the Add, Modify, Delete, and Test operations are not cached.

When enabled, the entire assembly line object is saved in the cache. The connection to the MySQL resource is maintained. The next request that the adapter receives can reuse this connection. Creating a new connection to the MySQL resource can take a lot of time. Caching data can save time and resource utilization.

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.

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

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

Installing the adapter language package

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

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

Related concepts

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

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

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

Related tasks

Installing the adapter binaries or connector

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

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

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

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

Verifying that the adapter is working correctly

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

Procedure

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

Related concepts

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

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

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

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

Related tasks

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

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

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

Chapter 4. Upgrading

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

To verify the required version of these adapter components, see the adapter release notes. For the installation steps, see Chapter 3, “Installing,” on page 7.

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 MySQL 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 MySQL Adapter compressed file that you downloaded from the IBM website. The 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`
- `erMySQLAccount.xml`
- `erMySQLService.xml`
- `MySQLAddUserAL.xml`
- `MySQLChangePasswordAL.xml`
- `MySQLDeleteUserAL.xml`
- `MySQLModifyUserAL.xml`
- `MySQLRestoreUserAL.xml`
- `MySQLSearch.xml`
- `MySQLSuspendUserAL.xml`
- `MySQLTest.xml`
- `schema.dsml`
- `service.def`

Procedure

- To edit the JAR file, take these steps:
  a) Log on to the workstation where the MySQL 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 MySQL Adapter profile. Type the name of the JAR file for your operating system.

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

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 MySQL 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 4 on page 23 contains warnings or errors that might be displayed in the user interface if the MySQL Adapter is installed on your system.

Table 4. Warning and error messages

Message code	Warning or error message	Remedial action
CTGIMT001E	The following error occurred. Error: Either the MySQL service name is incorrect or the service is not up.	Ensure that the MySQL service name given on IBM Security Verify Identity service form is running.
CTGIMT001E	The following error occurred. Error: Either the MySQL host or port is incorrect.	Verify that the host workstation name or the port for the MySQL 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.
CTGIMT004E	The adapter does not have permission to add an account: *Account_Name*.	The administrator user that is provided on the IBM Security Directory Integrator service form does not have the required privileges to add a user account. Ensure that an administrator user with the required privileges is specified on service form. These privileges are the minimum that are required for the administrator user: • CREATEROLE - Create Role permission • SUPERUSER - Superuser administrator authority
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

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.The MySQL adapter supports a standard set of attributes for user information.

The mandatory attribute to create an account is `User Name`

Table 5. Supported Account attributes

MySQL adapter attribute name	Description	Required
eruid	User Name	Yes
erPassword	Password for the user ID	No
erMySQLAuthType	Authentication type	No
erMySQLMaxQueries	Max queries	No
erMySQLMaxUpdates	Max updates	No
erMySQLMaxConnections	Max connections	No
erMySQLConConnection	Concurrent connection	No
erMySQLGlobalPrivileges	Global Privileges (Grant these privileges globally)	No
erMySQLRoles	Roles	No
erMySQLSchemaPrivs	Schema Privileges to Users	No

Table 6. Supported Role attributes

IBM MySQL adapter attribute name	Description	Required
erMySQLRoleName	Role Name	Yes
erMySQLRoleID	Role ID	No
erMySQLRoleDesc	Role Desc	No

Table 7. Supported Schema Privileges Attributes

IBM MySQL adapter attribute name	Description	Required
erMySQLSchemaID	Schema Name	No
erMySQLSchemaName	Schema ID	Yes
erMySQLSchemaDesc	Schema Desc	No

Table 8. Supported Schema Privileges Attributes		
IBM MySQL adapter attribute name	**Description**	**Required**
erMySQLGlobalPrivName	Global Schema Name	Yes
erMySQLGlobalPrivDesc	Global Schema Description	No

Table 9. Supported object classes	
Description	**Object class name in schema**
Service class	erMySQLService
Account class	erMySQLAccount
Role class	erMySQLRole
Schema class	erMySQLSchema
Global Privilege Class	erMySQLGlobalPriv

Adapter attributes by operations

Adapter attributes by operations refer to adapter actions by their functional transaction group. They are required for customization, creating provisioning rules, and understanding what service/target attributes are supported by the adapter.

System Login Add

A System Login Add is a request to create a user account with the specified attributes.

Table 10. Add request attributes	
Required attribute	**Optional attribute**
eruid	All other supported attributes

System Login Change

A System Login Change is a request to change one or more attributes for the specified users.

Table 11. Change request attributes	
Required attribute	**Optional attributes**
eruid	All other supported attributes

System Login Suspend

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

The user is not removed. User attributes are not modified. To Suspend the account, `connlimit` value is set to `0`.

Table 12. Suspend request attributes	
Required attribute	**Optional attribute**
eruid	None
erAccountStatus	None

System Login Restore

A System 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 is called. When `connlimit` value is set to `-1`, the user account is active.

Table 13. Restore attributes	
Required attribute	**Optional attribute**
eruid	None
erAccountStatus	None

Test

Use Test to verify the connection between the adapter and the Identity server.

Table 14. Test attributes	
Required attribute	**Optional attribute**
erMySQLServerHost	None
erMySQLServerPort	None
erMySQLDatabaseName	None
erserviceuid	None
erservicepwd1	None

Reconciliation

The Reconciliation request synchronizes user account information between IBM Security Verify Identity and the adapter.

Table 15. Reconciliation request attributes	
Required Attributes	**Optional Attributes**
None	All other supported Attributes

Adapter configuration properties

For information about setting Security Directory Integrator configuration properties for the operation of the MySQL adapter, see the *Dispatcher Installation and Configuration Guide*.

Special attributes

Certain attributes have special syntax and meaning that customers needs to be aware off. This information will be used to help the customer in how to supply the attribute value.This topic is not applicable for this adapter.

Index

A

adapter
- customization steps 19
- features 1
- installation
  - verifying 16
- installation worksheet 4
- profile
  - upgrading 17
- uninstall 25
- upgrading 17

adapter installation
- troubleshooting errors 21
- warnings 21

adapter overview 1
adapters
- removing profiles 25

add request attributes 28
attributes
- adapter action, by
  - adding 28
  - changing 28
  - modifying 28
  - pinging 29
- descriptions 27
- reconciliation 29

C

change request attributes 28

D

dispatcher
- installation 7
- upgrading 17

download, software 4

E

error messages 23

I

installation
- adapter 7
- adapter software 8
- first steps 19
- language pack 15
- planning roadmaps 3
- uninstall 25
- verification
  - adapter 16
- worksheet 4

L

language pack
- installation 15
- same for adapters and server 15

M

messages
- error 23
- warning 23

MS-DOS ASCII characters 20

O

operating system prerequisites 3
overview 1

P

ping request attributes 29
profile
- editing on UNIX or Linux 20

R

reconciliation attributes 29
removing
- adapter profiles 25

request attributes
- add 28
- change 28
- ping 29
- restore 29
- suspend 28

restore request attributes 29
roadmaps
- planning 3

S

service
- restart 9
- start 9
- stop 9

software
- download 4
- website 4

software requirements 3
suspend request attributes 28

T

troubleshooting
- error messages 23
- identifying problems 21

troubleshooting *(continued)*
    techniques for 21
    warning messages 23
troubleshooting and support
    troubleshooting techniques 21

U

uninstallation 25
updating
    adapter profile 19
upgrades
    adapter 17
    adapter profiles 17
    dispatcher 17

V

verification
    dispatcher installation 7
    installation 16
    operating system prerequisites 3
    operating system requirements 3
    software prerequisites 3
    software requirements 3
vi command 20

W

warning messages 23