IBM Security Verify Governance Identity Manager

SAP HANA Database Adapter Installation and Configuration Guide

IBM

Contents

Tables

Chapter 1. Overview

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

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

Features of the adapter

The adapter automates several administrative and management tasks.

The adapter automates these user account management tasks:

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

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

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

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

You must install the following components:

- 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.

describes the components that work together to complete the user account management tasks in a Security Directory Integrator environment.
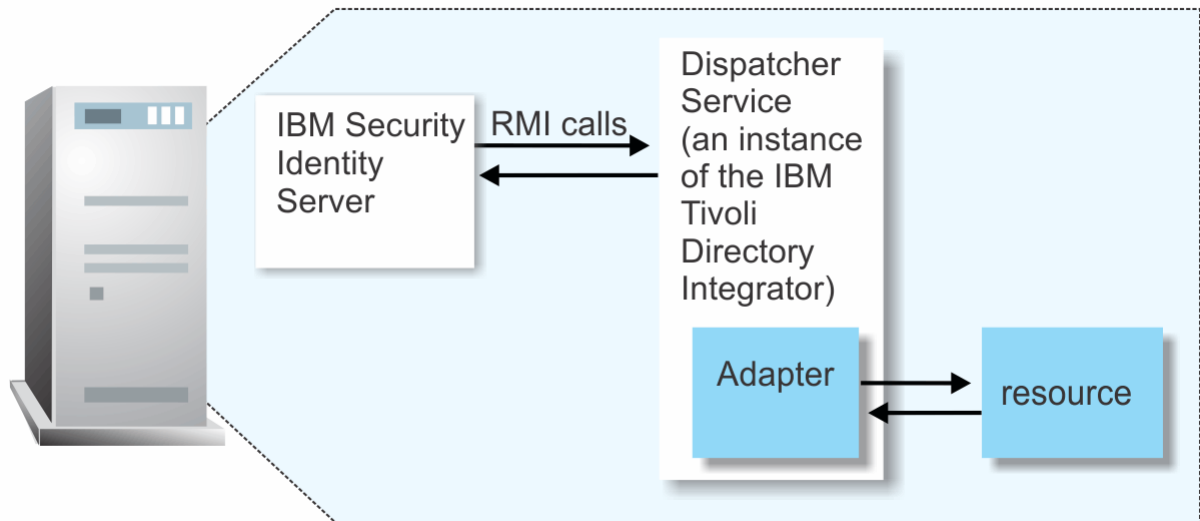
Figure 1. The architecture of the SAP HANA Database Adapter

Related concepts

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

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

The fundamental components in each environment are:

- 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
In a single server configuration, install the Identity server, the Security Directory Integrator server, and the SAP HANA Database Adapter on one server to establish communication with a SAP HANA Database. The SAP HANA Database is installed on a different server as described in .
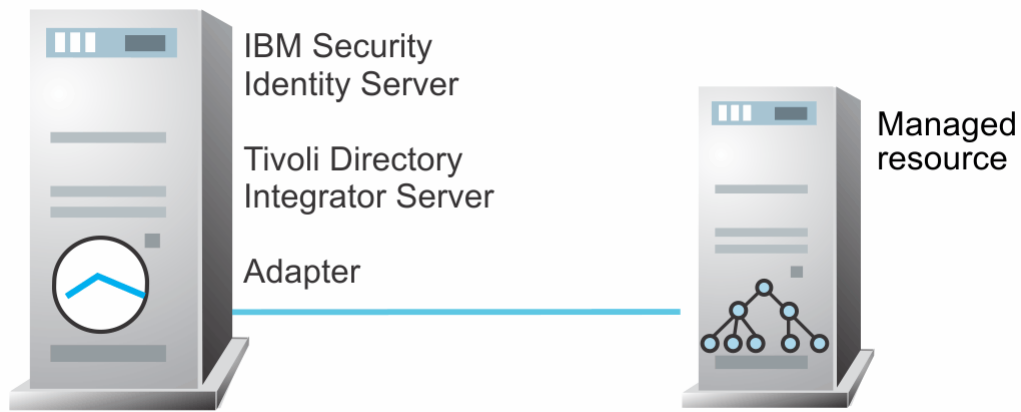
Figure 2. Example of a single server configuration

Multiple server configuration

In multiple server configuration, the Identity server, the Security Directory Integrator server, the SAP HANA Database Adapter, and the SAP HANA Database are installed on different servers. Install the Security Directory Integrator server and the SAP HANA Database Adapter on the same server as described in Figure 3 on page 3.

Figure 3. Example of multiple server configuration

Related concepts

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

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

Chapter 2. Planning

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

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

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

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

Pre-installation

Complete these tasks.

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

Installation

Complete these tasks.

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

Upgrade

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

Configuration

Complete these tasks.

1. Configure secure communication between the Identity server and the adapter.
   a. Configure 1-way authentication.
   b. Configure 2-way authentication.
2. Configure secure communication between the adapter and the managed target.
   a. Configure 1-way authentication.

b. Configure 2-way authentication.

3. Configure the adapter.

4. Modify the adapter profiles.

5. Customize the adapter.

Troubleshooting

See the following topics.

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

Uninstallation

Complete these tasks.

1. Stop the adapter service.

2. Remove the adapter binaries or connector.

3. Remove 3rd party client libraries.

4. Delete the adapter service/target.

5. Delete the adapter profile.

Reference

See the following topics.

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

Related concepts

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

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

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

Prerequisites

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

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
SAP HANA version	A system that runs the SAP HANA Database with SAP HANA Platf. Ed. 1.0 SPS09.
SAP HANA JDBC Driver	The driver file name is `ngdbc.jar`.
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.
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*.

Install the SAP HANA Database Adapter and place the appropriate SAP HANA JDBC driver into the Security Directory Integrator folder `[TDI_HOME]/jars/3rdparty/others`.

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

Related concepts

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

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

Installation worksheet

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

Software downloads

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

Go to IBM Passport Advantage.

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

Note:

You can also obtain additional adapter information from IBM Support.

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

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

Installation worksheet

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

Installation worksheet

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

Table 2. Required information to install the adapter		
Required information	**Description**	**Value**
IBM Security Directory Integrator Home Directory	The *ITDI_HOME* directory contains the jars/connectors subdirectory that contains adapter jars. For example, the jars/connectors subdirectory contains the jar for the UNIX adapter.	If Security Directory Integrator is automatically installed with your IBM Security Verify Governance Identity Manager product, the default directory path for Security Directory Integrator is as follows: **Windows:** • for version 7.1: *drive*\Program Files \IBM\TDI\V7.1 • for version 7.1.1 *drive*\Program Files \IBM\TDI\V7.1.1 **UNIX:** • for version 7.1: /opt/IBM/TDI/V7.1 • for version 7.1.1: /opt/IBM/TDI/V7.1.1

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 located at: **Windows:** • for version 7.1: *drive*\Program Files \IBM\TDI\V7.1*isimsoln* • for version 7.1.1: *drive*\Program Files \IBM\TDI \V7.1.1*isimsoln* **UNIX:** • for version 7.1: /opt/IBM/TDI/V7.1/ *isimsoln* • for version 7.1.1: /opt/IBM/TDI/V7.1.1/ *isimsoln*

Related concepts

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

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

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

Chapter 3. Installing in the Verify Governance Identity Manager virtual appliance

For Verify Governance Identity Manager target management, you can install an IBM Security Verify Adapters or a custom adapter on the built-in Security Directory Integrator in the virtual appliance instead of installing the adapter externally. As such, there is no need to manage a separate virtual machine or system.

About this task

This procedure is applicable for a selected list of Identity Adapters. See the Identity Adapters product documentation at http://www.ibm.com/support/knowledgecenter/SSIGMP_1.0.0/com.ibm.itim_pim.doc/c_adapters_intro.htm to determine which adapters are supported in Identity Governance and Intelligence, and which can be installed on the virtual appliance.

All Identity Governance and Intelligence supported adapters can be installed externally on the virtual appliance. Depending on the adapter, an external Security Directory Integrator may be required.

See the corresponding *Adapter Installation and Configuration Guide* for the specific prerequisites, installation and configuration tasks, and issues and limitations. See the *Adapters Release Notes* for any updates to these references.

Procedure

1. Download the adapter package from the IBM Passport Advantage.
   For example, Adapter-*<Adaptername>*.zip.

   The adapter package includes the following files:

Table 3. Adapter package contents	
Files	**Descriptions**
bundledefinition.json	The adapter definition file. It specifies the content of the package, and the adapter installation and configuration properties that are required to install and update the adapter.

Adapter JAR profile	An Security Directory Integrator adapter always include a JAR profile which contains:
	
	• targetProfile.json
	
	  – Service provider configuration
	  – Resource type configuration
	  – SCIM schema extensions
	  – List of assembly lines
	
	• A set of assembly lines in XML files
	• A set of forms in XML files
	• Custom properties that include labels and messages for supported languages.
	
	Use the **Target Administration** module to import the target profile.

Table 3. Adapter package contents (continued)

Files	Descriptions
Additional adapter specific files	Examples of adapter specific files: • Connector jar files • Configuration files • Script files • Properties files The file names are specified in the adapter definition file along with the destination directory in the virtual appliance.

2. From the top-level menu of the **Appliance Dashboard**, click **Configure** > **SDI Management**.

3. Select the instance of the Security Directory Integrator for which you want to manage the adapters and click **Manage** > **SDI Adapters**

   The **SDI Adapters** window is displayed with a table that list the name, version, and any comments about the installed adapters.

4. On the **SDI Adapters** window, click **Install**.

5. On the **File Upload** window, click **Browse** to locate the adapter package and then click **OK**.
   For example, Adapter-<*Adaptername*>.zip.

6. Provide the missing 3rd party libraries when prompted.

   a) On the **File Upload** for Pre-requisite files window, click **Select Files**.

      A new **File Upload** window is displayed.

   b) Browse and select all the missing libraries. For example, httpclient-4.0.1.jar

   c) Click **Open**.

      The selected files are listed in the **File Upload** for Pre-requisite files window.

   d) Click **OK**.

      The missing files are uploaded and the adapter package is updated with the 3rd party libraries.

7. Enable secure communication.

   a) Select the instance of the Security Directory Integrator for which you want to manage the adapter.

   b) Click **Edit**.

   c) Click the **Enable SSL** check box.

   d) Click **Save Configuration**.

8. Import the SSL certificate to the IBM Security Directory Integrator server.

   a) Select the instance of the Security Directory Integrator for which you want to manage the adapter.

   b) Click **Manage** > **Certificates**.

   c) Click the **Signer** tab.

   d) Click **Import**.

      The **Import Certificate** window is displayed.

   e) Browse for the certificate file.

   f) Specify a label for the certificate. It can be any name.

   g) Click **Save**.

Chapter 4. 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.

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
You can import a profile definition file, which creates a profile in Identity server. Use this option for importing adapter profiles.

Importing attribute mapping file
After importing the adapter profile, you must import an attribute map from a profile mapping definition file.

Adding a connector
After you import the adapter profile on the Verify Governance Identity Manager server, add a connector so that Verify Governance Identity Manager server can communicate with the managed resource.

Enabling connectors
After you create a connector, by default it is in a disabled state. You must enable a connector to use it.

Reviewing and setting channel modes for each new connector
Use this procedure to set up the read-from and write-to channels and to set the synchronization schedule for each new connector.

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.

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.

Related tasks

Importing the adapter profile
You can import a profile definition file, which creates a profile in Identity server. Use this option for importing adapter profiles.

Importing attribute mapping file
After importing the adapter profile, you must import an attribute map from a profile mapping definition file.

Adding a connector
After you import the adapter profile on the Verify Governance Identity Manager server, add a connector so that Verify Governance Identity Manager server can communicate with the managed resource.

Enabling connectors
After you create a connector, by default it is in a disabled state. You must enable a connector to use it.

Reviewing and setting channel modes for each new connector
Use this procedure to set up the read-from and write-to channels and to set the synchronization schedule for each new connector.

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.

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.

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
You can import a profile definition file, which creates a profile in Identity server. Use this option for importing adapter profiles.

Importing attribute mapping file
After importing the adapter profile, you must import an attribute map from a profile mapping definition file.

Adding a connector
After you import the adapter profile on the Verify Governance Identity Manager server, add a connector so that Verify Governance Identity Manager server can communicate with the managed resource.

Enabling connectors
After you create a connector, by default it is in a disabled state. You must enable a connector to use it.

Reviewing and setting channel modes for each new connector
Use this procedure to set up the read-from and write-to channels and to set the synchronization schedule for each new connector.

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.

Importing the adapter profile

You can import a profile definition file, which creates a profile in Identity server. Use this option for importing adapter profiles.

Before you begin

• The Identity server is installed and running.

- You have 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.

About this task

Target definition files are also called adapter profile files. The profile definition files are provided with the various IBM Security Verify Adapter. The adapter profile must be imported because it defines the types of resources that the Verify Governance Identity Manager server can manage.

The adapter profile definition file is used to create a target profile on the Verify Governance Identity Manager server and to establish communication with the adapter. If the adapter profile is not imported, you cannot create a connector for that adapter type.

An upload error might occur when no file is selected, or when the file is empty, or due to any upload operation error, such as a timeout or connection error. If the adapter profile is not installed correctly, the adapter cannot function correctly. You cannot create a connector with the adapter profile or open and account on the service. You must import the adapter profile again.

This task can be completed from the Enterprise Connectors module in the Administration Console. To import an adapter target profile, complete these steps:

Procedure

1. Log in to the Verify Governance Identity Manager Administration Console.
2. From the Administration Console, select **Enterprise Connectors**.
3. Select **Manage** > **Profiles**.
4. Optional: Click **Filter** to toggle the filter on to refine your search results, or click **Hide Filter** to toggle the filter off. When the filter is visible, you can specify search criteria for your requests, and then click **Search**.
5. Click **Actions** > **Import**.
6. On the **Import** page, complete these steps:
   a) Select **Profile**.
   b) Click **Browse** to locate the JAR file that you want to import.
   c) Click **Upload file**.
      A message indicates that you successfully imported a profile.
7. Click **Close**.
   The new profile is displayed in the list of profiles.

Results

The upload is synchronous but has a timeout. The progress bar on the **Import** page accurately indicates the upload status. However, when a timeout is reached, the following message occurs: "The import is still in progress and will complete shortly. Close this window to proceed." If you see that message, allow a few minutes for the upload to complete and for the profile to be available.

What to do next

After the target profile is imported successfully, complete these tasks.

- Import the attribute mapping file. See "Importing attribute mapping file" on page 17.
- Create a connector that uses the target profile. See "Adding a connector" on page 18.

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 attribute mapping file
After importing the adapter profile, you must import an attribute map from a profile mapping definition file.

Adding a connector
After you import the adapter profile on the Verify Governance Identity Manager server, add a connector so that Verify Governance Identity Manager server can communicate with the managed resource.

Enabling connectors
After you create a connector, by default it is in a disabled state. You must enable a connector to use it.

Reviewing and setting channel modes for each new connector
Use this procedure to set up the read-from and write-to channels and to set the synchronization schedule for each new connector.

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.

Importing attribute mapping file

After importing the adapter profile, you must import an attribute map from a profile mapping definition file.

About this task

This task involves importing an account attribute mapping definition file, which is included in the adapter package. The imported file must be a DEF file.

Procedure

1. Log in to the Verify Governance Identity Manager Administration Console.
2. From the Administration Console, select **Enterprise Connectors**.
3. Select **Manage** > **Profiles**.
4. Optional: Click **Filter** to toggle the filter on to refine your search results, or click **Hide Filter** to toggle the filter off. When the filter is visible, you can specify search criteria for your requests, and then click **Search**.
5. Click **Actions** > **Import**.
6. On the **Import** page, complete these steps:

    a) Select **Attribute Mapping**.

b) Click **Browse** to locate the attribute mapping file that you want to import.

c) Click **Upload file**.

A message indicates that you successfully imported the file.

7. Click **Close**.

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
You can import a profile definition file, which creates a profile in Identity server. Use this option for importing adapter profiles.

Adding a connector
After you import the adapter profile on the Verify Governance Identity Manager server, add a connector so that Verify Governance Identity Manager server can communicate with the managed resource.

Enabling connectors
After you create a connector, by default it is in a disabled state. You must enable a connector to use it.

Reviewing and setting channel modes for each new connector
Use this procedure to set up the read-from and write-to channels and to set the synchronization schedule for each new connector.

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.

Adding a connector

After you import the adapter profile on the Verify Governance Identity Manager server, add a connector so that Verify Governance Identity Manager server can communicate with the managed resource.

Before you begin

Complete Importing the adapter profile.

Note: If you migrated from Verify Governance Identity Manager V5.2.2 or V5.2.2.1 and want to add or configure a connector, see *Adding and configuring a connector for each target* in the IBM Security Verify Governance Identity Manager product documentation.

About this task

The connectors consolidate, extract, and reconcile user identities, organization units, permissions, and user entitlements with the most common enterprise applications. Configure a connector to keep the Access Governance Core repository synchronized with the target system.

This task can be completed from the Enterprise Connectors module in the Administration Console.

Procedure

To add a connector, complete these steps.
1. Log in to the Verify Governance Identity Manager Administration Console.
2. From the Administration Console, select **Enterprise Connectors**.
3. Select **Manage** > **Connectors**.

   A list of connectors is displayed on the **Connectors** tab.
4. Click **Filter** to toggle the filter on to refine your search results, or click **Hide Filter** to toggle the filter off. When the filter is visible, you can specify search criteria for your requests, and then click **Search**.
5. To view all of the columns in the list of connectors, expand the **Connectors** pane.
6. Click **Actions** > **Add**.

   The **Connector Details** pane is enabled for your input.
7. On the **Connector Details** tab, complete these steps:
   a) Assign a name and description for the connector.
   b) Select the target profile type as `Identity Brokerage` and its corresponding target profile.
   c) Select the entity, such as **Account** or **User**.

      Depending on the connector type, this field might be preselected.
   d) Optional: Select **Trace ON** and the corresponding **Trace Level** to enable trace logs.

      The available trace levels are DEBUG, INFO, and ERROR.
   e) Optional: Select **History ON** to save and track the connector usage.
   f) Click **Save**.

      The fields for enabling the channels for sending and receiving data are now visible.
   g) Select and set the connector properties in the **Global Config** accordion pane.

      For information about the global configuration properties, see Global Config accordion pane.
   h) Click **Save**. The fields for enabling the channels for sending and receiving data are now visible.

Results

The connector is saved and added to the list of connectors in the **Connectors** pane.

If you cannot create a connector with the target profile or open an account on an existing connector, the target profile was not installed correctly during the import. You must import the target profile again.

What to do next

Enable the channel modes to synchronize the data between the target systems and Verify Governance Identity Manager. For more information, see "Enabling connectors" on page 20.

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
You can import a profile definition file, which creates a profile in Identity server. Use this option for importing adapter profiles.

Importing attribute mapping file
After importing the adapter profile, you must import an attribute map from a profile mapping definition file.

Enabling connectors
After you create a connector, by default it is in a disabled state. You must enable a connector to use it.

Reviewing and setting channel modes for each new connector
Use this procedure to set up the read-from and write-to channels and to set the synchronization schedule for each new connector.

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.

Enabling connectors

After you create a connector, by default it is in a disabled state. You must enable a connector to use it.

Before you begin

Table 4. Prerequisites for enabling a connector	
Prerequisite	**Find more information**
A connector must exist in Verify Governance Identity Manager.	"Adding a connector" on page 18.
Ensure that you enabled the appropriate channel modes for the connector.	"Reviewing and setting channel modes for each new connector" on page 22.

Procedure

To enable a connector, complete these steps:

1. Log in to the Verify Governance Identity Manager Administration Console.
2. From the Administration Console, select **Enterprise Connectors**.
3. Select **Manage** > **Connectors**.

   A list of connectors is displayed on the **Connectors** tab.
4. Optional: Click **Filter** to toggle the filter on to refine your search results, or click **Hide Filter** to toggle the filter off. When the filter is visible, you can specify search criteria for your requests, and then click **Search**.

5. Optional: To view all of the columns in the list of connectors, expand the **Connectors** pane.
6. Select the connector that you want to enable.
7. On the **Connector Details** tab, complete these steps:

    a) Select the channel modes that you want to enable, and then click **Save**. Depending on the channels that you enable, the corresponding **Channel** tabs are displayed.

    Enable write-to channel
    > Propagates every change in the Access Governance Core repository into the target system.
    >
    > For connectors that are not HR feed, the check boxes for enabling the read-from channel and the write-to channel are available.

    Enable read-from channel
    > Reads the INPUT EVENTS and USER DATA from the target system. Imports data from the target system to the Access Governance Core repository.
    >
    > For HR feed connectors, only the check box for enabling the read-from channel is available.

    Enable reconciliation
    > Synchronizes the modified data between the Access Governance Core repository and the target system.

Results

The connector is enabled

What to do next

Enable the channel modes to synchronize the data between the target systems and Verify Governance Identity Manager.

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
You can import a profile definition file, which creates a profile in Identity server. Use this option for importing adapter profiles.

Importing attribute mapping file
After importing the adapter profile, you must import an attribute map from a profile mapping definition file.

Adding a connector
After you import the adapter profile on the Verify Governance Identity Manager server, add a connector so that Verify Governance Identity Manager server can communicate with the managed resource.

Reviewing and setting channel modes for each new connector

Use this procedure to set up the read-from and write-to channels and to set the synchronization schedule for each new connector.

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.

Reviewing and setting channel modes for each new connector

Use this procedure to set up the read-from and write-to channels and to set the synchronization schedule for each new connector.

About this task

Note: Legacy Verify Governance Identity Manager Enterprise connectors use `Reconciliation` channel, whereas Identity Brokerage Enterprise connectors use `Read From Channel` and `Change Log Sync`.

For more information about any of tasks in the following steps, see the IBM® Security Identity Governance and Intelligence product documentation.

Procedure

To enable the read-from and write-to channels, and to set the change log synchronization schedule for each new connector, complete these steps in Verify Governance Identity Manager V5.2.3:

1. Log in to the Verify Governance Identity Manager Administration Console.
2. From the Administration Console, select **Enterprise Connectors**.
3. Select **Manage** > **Connectors**.

   A list of connectors is displayed on the **Connectors** tab.
4. Optional: Click **Filter** to toggle the filter on to refine your search results, or click **Hide Filter** to toggle the filter off. When the filter is visible, you can specify search criteria for your requests, and then click **Search**.
5. Optional: To view all of the columns in the list of connectors, expand the **Connectors** pane.
6. Select the connector that you want to enable.
7. On the **Connector Details** tab, complete these steps:
   a) Select the channel modes that you want to enable, and then click **Save**. Depending on the channels that you enable, the corresponding **Channel** tabs are displayed, in which you can do more configuration, such as mapping attributes and setting up rules.

      Enable write-to channel
         Propagates every change in the Access Governance Core repository into the target system.

      Enable read-from channel
         Reads the INPUT EVENTS and USER DATA from the target system. Imports data from the target system to the Access Governance Core repository.

      Enable reconciliation
         Synchronizes the modified data between the Access Governance Core repository and the target system.
8. Select **Monitor** > **Change Log Sync Status**.

   A list of connectors is displayed.
9. On the **Change Log Sync Status** tab, complete these steps:
   a) Optional: Click **Filter** to toggle the filter on to refine your search results, or click **Hide Filter** to toggle the filter off. When the filter is visible, you can specify search criteria for your requests, and then click **Search**.

b) Select a connector, and click **Actions** > **Sync Now**.

   The synchronization process begins.

   c) Optional: To view the status of the synchronization request, select **Sync History** in the right pane.

   Information about the synchronization is displayed in the **Sync History** tab.

10. Set the change log synchronization schedule for each new connector that you migrated.

11. When the connector configuration is complete, enable the connector by completing these steps:

   a) Select **Manage** > **Connectors**.

   b) Select the connector that you want to enable, and then select the **Enable** check box in the **Connector Details** tab.

   c) Click **Save**.

   For more information, see "Enabling connectors" on page 20.

   For Identity Brokerage connectors that are not HR feed, the check boxes for enabling the read-from channel and the write-to channel are available.

   For Identity Brokerage HR feed connectors, only the check box for enabling the read-from channel is available.

12. Start the connector by selecting **Monitor** > **Connector Status**. Select the connector that you want to start, and then select **Actions** > **Start**.

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
You can import a profile definition file, which creates a profile in Identity server. Use this option for importing adapter profiles.

Importing attribute mapping file
After importing the adapter profile, you must import an attribute map from a profile mapping definition file.

Adding a connector
After you import the adapter profile on the Verify Governance Identity Manager server, add a connector so that Verify Governance Identity Manager server can communicate with the managed resource.

Enabling connectors
After you create a connector, by default it is in a disabled state. You must enable a connector to use it.

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.

Attribute Mapping

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

About this task

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

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

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

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

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

Note:

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

Procedure

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

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

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

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

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

Attribute	Mapped Attribute
eruid	CODE
erpassword	PASSWORD

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

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
You can import a profile definition file, which creates a profile in Identity server. Use this option for
importing adapter profiles.

Importing attribute mapping file
After importing the adapter profile, you must import an attribute map from a profile mapping definition
file.

Adding a connector
After you import the adapter profile on the Verify Governance Identity Manager server, add a connector so
that Verify Governance Identity Manager server can communicate with the managed resource.

Enabling connectors
After you create a connector, by default it is in a disabled state. You must enable a connector to use it.

Reviewing and setting channel modes for each new connector
Use this procedure to set up the read-from and write-to channels and to set the synchronization schedule
for each new connector.

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.

The accounts must be able to remotely connect to the SAP HANA Database server and must have
sufficient privileges to administer the SAP HANA Database users.

Table 5. Required privileges and their descriptions	
Privilege	**Description**
sap.hana.admin.roles.Administrator	Administer the SAP HANA Database users.

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.

Note: If the following fields on the service form are changed for an existing service, the adapter service on
the Security Directory Integrator server must be restarted.

- **Service Name**
- **Password**
- **AL FileSystem Path**

- **Max Connection Count**

On the SAP HANA 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`.

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

Table 6. Ports	
Instance	**Ports**
SDI1	1199, 1198, 1197, 1196, 1195, 1194
SDI2	2299, 2298, 2297, 2296, 2295, 2294
SDI3	3399, 3398, 3397, 3396, 3395, 3394
SDI4	4499, 4498, 4497, 4496, 4495, 4494
SDI5	5599, 5598, 5597, 5596, 5595, 5594
SDI6	6699, 6698, 6697, 6696, 6695, 6694
SDI7	7799, 7798, 7797, 7796, 7795, 7794
SDI8	8899, 8898, 8897, 8896, 8895, 8894
SDI9	9999, 9998, 9997, 9996, 9995, 9994
SDI10	11099, 11098, 11097, 11096, 11095, 11094

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

- 1099
- 2099
- 3099

SAP HANA Service Name
Specify the service name of the SAP HANA instance to which the adapter must connect.

SAP HANA Service URL
Specify the URL and port number on which the SAP HANA service is listening.

For example: `jdbc:sap://myServer:30015` (The port should be 3<instance number> 15, for example, 30015, if the instance is 00)

SAP HANA Administrator Name
Specify the name of the user who has access to the SAP HANA resource and can do administrative operations.

SAP HANA Administrator Password
Specify the password for the user.

Owner
Optional: 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 FileSystem Path
Specify the file path from where the dispatcher loads the assembly lines. If you do not specify a file path, the dispatcher loads the assembly lines that are received from Identity server. For example, you can specify the following file path to load the assembly lines from the `profiles` directory of the Windows operating system: `c:\Files\IBM\TDI\V7.0\profiles` or you can specify the following file path to load the assembly lines from the `profiles` directory of the UNIX and Linux® operating system: `system:/opt/IBM/TDI/V7.0/profiles`.

Max Connection Count
Specify the maximum number of assembly lines that the dispatcher can run simultaneously for the service. For example, enter `10` when 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
This page contains read-only information about the adapter and the managed resource. These fields are examples. The actual fields vary depending on the type of adapter and how the service form is configured. The adapter must be running to obtain the information. Click **Test Connection** to populate the fields.

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

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

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

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

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

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

Dispatcher version
Specifies the version of the Dispatcher.

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

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

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

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

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

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

- Verify the adapter log to ensure that the test request was successfully sent to the adapter.
- Verify the adapter configuration information.
- Verify the service parameters for the adapter profile. For example, verify the workstation 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.

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
You can import a profile definition file, which creates a profile in Identity server. Use this option for importing adapter profiles.

Importing attribute mapping file
After importing the adapter profile, you must import an attribute map from a profile mapping definition file.

Adding a connector
After you import the adapter profile on the Verify Governance Identity Manager server, add a connector so that Verify Governance Identity Manager server can communicate with the managed resource.

Enabling connectors
After you create a connector, by default it is in a disabled state. You must enable a connector to use it.

Reviewing and setting channel modes for each new connector
Use this procedure to set up the read-from and write-to channels and to set the synchronization schedule for each new connector.

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.

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.

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
You can import a profile definition file, which creates a profile in Identity server. Use this option for importing adapter profiles.

Importing attribute mapping file
After importing the adapter profile, you must import an attribute map from a profile mapping definition file.

Adding a connector
After you import the adapter profile on the Verify Governance Identity Manager server, add a connector so that Verify Governance Identity Manager server can communicate with the managed resource.

Enabling connectors
After you create a connector, by default it is in a disabled state. You must enable a connector to use it.

Reviewing and setting channel modes for each new connector
Use this procedure to set up the read-from and write-to channels and to set the synchronization schedule for each new connector.

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

Chapter 5. 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 4, "Installing," on page 13.

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 6. Configuring

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

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

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

Customizing the adapter profile

To customize the adapter profile, you must modify the SAP HANA Database 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.

The JAR file is included in the SAP HANA Database 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`
- `erHANAAccount.xml`
- `erHANARMIService.xml`
- `AddHanaAcc.xml`
- `DeleteHanaAcc.xml`
- `AlterHanaAcc.xml`
- `SearchHanaAcc.xml`
- `TestHanaConnection.xml`
- `service.def`
- `schema.dsml`

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

Procedure

1. Edit the JAR file.
   a) Log on to the workstation where the SAP HANA Database Adapter is installed.
   b) On the **Start** menu, select **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 SAP HANA Database Adapter profile. Type the name of the JAR file for your operating system.

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

2. Import the file.

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

Run the following commands:

Windows

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

UNIX

```
jar -cvf HANAAdapterProfile.jar HANAAdapterProfile
```

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

c) Stop and start the Identity server.

d) Restart the adapter service.

Related concepts

Configuration properties of the Dispatcher
The `solution.properties` file and the `itim_listener.properties` file contain the configuration properties for the Dispatcher.

Enabling SSL communication
You can secure your environment with SSL communication between IBM Security Verify Governance Identity Manager, and Security Directory Integrator.

Password management for account restoration
How each restore action interacts with its corresponding managed resource depends on the managed resource or on the business processes that you implement.

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.

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

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 concepts

Configuration properties of the Dispatcher
The solution.properties file and the itim_listener.properties file contain the configuration properties for the Dispatcher.

Enabling SSL communication
You can secure your environment with SSL communication between IBM Security Verify Governance Identity Manager, and Security Directory Integrator.

Password management for account restoration
How each restore action interacts with its corresponding managed resource depends on the managed resource or on the business processes that you implement.

Related tasks

Customizing the adapter profile
To customize the adapter profile, you must modify the SAP HANA Database Adapter JAR file. You might customize the adapter profile to change the account form or the service form.

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

Configuration properties of the Dispatcher

The solution.properties file and the itim_listener.properties file contain the configuration properties for the Dispatcher.

To configure the dispatcher properties, follow the configuration instructions included in the dispatcher download package.

Related concepts

Enabling SSL communication
You can secure your environment with SSL communication between IBM Security Verify Governance Identity Manager, and Security Directory Integrator.

Password management for account restoration
How each restore action interacts with its corresponding managed resource depends on the managed resource or on the business processes that you implement.

Related tasks

Customizing the adapter profile
To customize the adapter profile, you must modify the SAP HANA Database Adapter JAR file. You might customize the adapter profile to change the account form or the service form.

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.

Verifying that the adapter is working correctly

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

Enabling SSL communication

You can secure your environment with SSL communication between IBM Security Verify Governance Identity Manager, and Security Directory Integrator.

To use SSL communication between the system components, you can configure the Security Directory Integrator server as the SSL server.

The main communication channel that you can secure with SSL communication is depicted in Figure 1
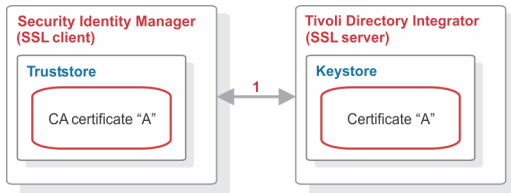

Figure 4. SSL Communication Overview

This channel includes communication between IBM Security Verify Governance Identity Manager and Security Directory Integrator. To configure SSL communication for this channel, see the Secure Sockets Layer (SSL) information in the *IBM Security Dispatcher Installation and Configuration Guide*.

Related concepts

Configuration properties of the Dispatcher
The `solution.properties` file and the `itim_listener.properties` file contain the configuration properties for the Dispatcher.

Password management for account restoration
How each restore action interacts with its corresponding managed resource depends on the managed resource or on the business processes that you implement.

Related tasks

Customizing the adapter profile
To customize the adapter profile, you must modify the SAP HANA Database Adapter JAR file. You might customize the adapter profile to change the account form or the service form.

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.

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

Password management for account restoration

How each restore action interacts with its corresponding managed resource depends on the managed resource or on the business processes that you implement.

Certain resources reject a password when a request is made to restore an account. In this case, you can configure IBM Security Verify Governance Identity Manager to forego the new password requirement. You can configure the SAP HANA Database Adapter to require a new password when the account is restored. This feature is useful if your company's business processes require you to reset the password when an account is restored.

In the `service.def` file, you can define whether a password is required as a new protocol option. When you import the adapter profile, if an option is not specified, the adapter profile importer determines the correct restoration password behavior from the `schema.dsml` file. The adapter profile components enable remote services to know whether to discard a password that is entered by the user where multiple accounts on disparate resources are being restored. In this situation, where only some of the accounts

that are being restored might require a password. Remote services discard the password from the restore action for those managed resources that do not require them.

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

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

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

Related concepts

Configuration properties of the Dispatcher
The `solution.properties` file and the `itim_listener.properties` file contain the configuration properties for the Dispatcher.

Enabling SSL communication
You can secure your environment with SSL communication between IBM Security Verify Governance Identity Manager, and Security Directory Integrator.

Related tasks

Customizing the adapter profile
To customize the adapter profile, you must modify the SAP HANA Database Adapter JAR file. You might customize the adapter profile to change the account form or the service form.

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.

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

Configuration properties of the Dispatcher
The `solution.properties` file and the `itim_listener.properties` file contain the configuration properties for the Dispatcher.

Enabling SSL communication
You can secure your environment with SSL communication between IBM Security Verify Governance Identity Manager, and Security Directory Integrator.

Password management for account restoration
How each restore action interacts with its corresponding managed resource depends on the managed resource or on the business processes that you implement.

Related tasks

Customizing the adapter profile

To customize the adapter profile, you must modify the SAP HANA Database Adapter JAR file. You might customize the adapter profile to change the account form or the service form.

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.

Chapter 7. 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 need to know about the adapter or about an error. Table 7 on page 41 contains warnings or errors which might be displayed in the user interface if the SAP HANA Database Adapter is installed on your system.

Table 7. Warning and error messages

Message code	Warning or error message	Remedial action
CTGIMT001E	The following error occurred. Error: Either the SAP HANA service name is incorrect or the service is not up.	Ensure that the SAP HANA service name that is provided on the IBM Security Verify Governance Identity Manager service form is running.
CTGIMT001E	The following error occurred. Error: Either the SAP HANA host or port is incorrect.	Verify that the host workstation name or the port for the SAP HANA service is correctly specified.
CTGIMT002E	The login credential is missing or incorrect.	Verify that you provided correct login credential on the service form.
CTGIMT001E	The following error occurred. Error: No suitable JDBC driver found.	Ensure that the correct version of the JDBC thin 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 Governance Identity Manager 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 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.
CTGIMT003E	The account already exists.	Use 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 8. 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.

Uninstalling the adapter

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

About this task

The SAP HANA Database Adapter installation installs the Dispatcher only on the Security Directory Integrator server. Therefore, you only need to uninstall from the Dispatcher. There is no uninstall for the SAP HANA Database Adapter.

The JAR file needed to uninstall the Dispatcher was created in the *ITDI_HOME*\DispatcherUninstall directory when the Dispatcher was installed.

Note: The Dispatcher is required for all Security Directory Integrator-based adapters. If you uninstall the Dispatcher, none of the other installed adapters function.

To remove the SAP HANA Database Adapter, complete these steps:

1. Stop the adapter service.
2. Run the `DispatcherUninstall.jar` file. To run the JAR file, double-click on the executable file or enter the following command at the command prompt:

   ```
   TDI_HOME/jvm/jre/bin/java  -jar  DispatcherUninstall.jar
   ```

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

Deleting the adapter profile

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

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

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

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

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

Related tasks
Uninstalling the adapter

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

Chapter 9. Reference

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

Adapter attributes and object classes

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

The combination of attributes that is included in the packets depend on the type of action that the Identity server requests from the SAP HANA Database Adapter.

Table 8 on page 45 is a listing of the attributes that are used by the SAP HANA Database Adapter. The table gives a brief description and corresponding column on the SAP HANA Database (if applicable) for the value of the attribute.

Table 8. Attributes, object identifiers, descriptions, and corresponding column/table name on the SAP HANA Database

Attribute	Description
erhanaservicename	SAP HANA Service
erhanaaccount	SAP HANA Account
erhanarmiservice	SAP HANA Service
HANAadapterProfile	SAP HANA Profile
HANAAdapterProfileDesc	SAP HANA Service Profile
erhanasamloption	SAML
erhanax509certoption	X509
erhanasaplogonticketoption	SAP Logon Ticker
erhanasapassertionoption	SAP Assertion Ticker
erhanakerberosoption	Kerberos
erhanaexternalid	External ID*
erhanavalidfrom	Valid From
erhanavaliduntil	Valid Until
erhanasessionclient	Session Client
erhanarolenames	Role

Table 8. Attributes, object identifiers, descriptions, and corresponding column/table name on the SAP HANA Database (continued)

Attribute	Description
erhanasystemprivnames	System Privileges
erhanacatobjnames	Catalog Object
erhanaanalyticprivnames	Analytic Privileges
erhanapackagenames	Package Name
erhanaappsprivnames	Application Privileges
erhanaprivonusersnames	User
erhanauserparamnames	User Parameters This is a multi-valued attribute. Each value consists of two fields: the "Parameter name" and the "Parameter value" separated by the vertical bar character: Parameter|Value
erhanasamlidentities	External SAML Identities This is a multi-valued attribute. Each value consists of two fields: the "SAML provider name" and the "external identity" separated by the vertical bar character: provider|identity
erhanax509certmappings	X509 User Certificates This is a multi-valued attribute. Each value consists of two fields: the "Issued to" and the "Issued by" separated by the vertical bar character: Issued To|Issued By
erhanaalfilesystempath	FileSystem Path to SDI AssemblyLines for HANA
erhanaservicehost	SAP HANA Service URL
erServiceUid	The SAP HANA resource administrator ID.
erPassword	The password for SAP HANA administrator.
erUid	The login name.
erAccountStatus	The status of the account either enabled or disabled.

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.

The topics include more information about required and optional attributes sent to the SAP HANA Database Adapter to complete that action.

System Login Add

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

Table 9. Add request attributes for SAP HANA	
Required attribute	**Optional attribute**
erUid	All other supported attributes

Related concepts

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

System Login Delete
A System Login Delete is a request to remove the specified user from the SAP HANA Database.

System Login Suspend
A System Login Suspend is a request to disable a user account. The user is not removed, and the user's attributes are not modified.

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 was called.

Test
You can use attributes to test the connection.

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

System Login Change

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

Table 10. Change request attributes for SAP HANA	
Required attribute	**Optional attribute**
erUid	All other supported attributes

Related concepts

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

System Login Delete
A System Login Delete is a request to remove the specified user from the SAP HANA Database.

System Login Suspend
A System Login Suspend is a request to disable a user account. The user is not removed, and the user's attributes are not modified.

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 was called.

Test
You can use attributes to test the connection.

Reconciliation

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

System Login Delete

A System Login Delete is a request to remove the specified user from the SAP HANA Database.

Table 11. Delete request attributes for SAP HANA	
Required attribute	**Optional attribute**
erUid	None

Related concepts

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

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

System Login Suspend
A System Login Suspend is a request to disable a user account. The user is not removed, and the user's attributes are not modified.

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 was called.

Test
You can use attributes to test the connection.

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

System Login Suspend

A System Login Suspend is a request to disable a user account. The user is not removed, and the user's attributes are not modified.

Table 12. Suspend request attributes for SAP HANA	
Required attribute	**Optional attribute**
erUid	None
erAccountStatus	

Related concepts

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

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

System Login Delete
A System Login Delete is a request to remove the specified user from the SAP HANA Database.

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 was called.

Test
You can use attributes to test the connection.

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

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 was called.

Table 13. Restore request attributes for SAP HANA	
Required attribute	**Optional attribute**
erUid erAccountStatus	None

Related concepts

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

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

System Login Delete
A System Login Delete is a request to remove the specified user from the SAP HANA Database.

System Login Suspend
A System Login Suspend is a request to disable a user account. The user is not removed, and the user's attributes are not modified.

Test
You can use attributes to test the connection.

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

Test

You can use attributes to test the connection.

Table 14. Test attributes	
Required attribute	**Optional attribute**
None	None

Related concepts

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

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

System Login Delete

A System Login Delete is a request to remove the specified user from the SAP HANA Database.

System Login Suspend
A System Login Suspend is a request to disable a user account. The user is not removed, and the user's attributes are not modified.

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 was called.

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

Reconciliation

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

Table 15. Reconciliation request attributes for SAP HANA	
Required attribute	**Optional attribute**
None	None

Related concepts

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

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

System Login Delete
A System Login Delete is a request to remove the specified user from the SAP HANA Database.

System Login Suspend
A System Login Suspend is a request to disable a user account. The user is not removed, and the user's attributes are not modified.

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 was called.

Test
You can use attributes to test the connection.

Index

P

private key, definition 36
profile
    editing on UNIX or Linux 34
properties
    configuring the Dispatcher 35
protocol
    SSL, overview 36

R

Reconciliation request 50
removing
    adapter profiles 43
requests
    Reconciliation 50
    System Login Add 47
    System Login Change 47
    System Login Delete 48
    System Login Restore 49
    System Login Suspend 48
roadmaps
    planning 5

S

service
    restart 15
    start 15
    stop 15
software
    download 8
    requirements 6
    website 8
SSL
    certificate installation 36
    overview 36
System Login Add request 47
System Login Change request 47
System Login Delete request 48
System Login Restore request 49
System Login Suspend request 48

T

troubleshooting
    error messages 41
    identifying problems 39
    techniques for 39
    warning messages 41
troubleshooting and support
    troubleshooting techniques 39

U

uninstallation 43
uninstalling, adapter from the directory integrator 43
upgrades
    adapter 31
    adapter profile 33
    adapter profiles 31
    dispatcher 31

user account
    Reconciliation 50

V

verification
    dispatcher installation 13
    installation 37
    operating system prerequisites 6
    software prerequisites 6
vi command 34

W

warning messages 41

IBM®